HOME: CYBER CRIME INDIA

An Information Technology blog by the Convenor of India's Public Law Initiative. This weblog is about Computer Hacking, Credit Card Fraud, and Foreign Banks illegally functioning in India. Sarbajit Roy has filed India's first IT ACT 2000 Cyber Crime Complaint on rampant Hacking widespread in India's Banking, Financial and BPO sectors, inter-alia seeking imprisonment of Senior Officials of the Reserve Bank of India (RBI) and Credit Information Bureau (India) Ltd (CIBIL) for criminal complicity.

FILES

ALL BLOG POSTS

ZONES

Master Plan of Delhi 2021

LINKS

Sarbajit Roy

PREVIOUS 10 POSTS

This "popular" blog makes it to national print med...

Sarbajit puts Delhi Govt in "legal fix"

Sarbajit versus Goliath.

DERC faces contempt petition [Sarbajit Roy]

Sarbajit and his multicoloured RTI raincoat

RTI: Depts have put up manuals online

Central Information Commission to hear first case ...

2005, Right to Information Act gets 1st applicant

Pawan Duggal comments Ebay India PaisaPay encrypti...

another example of the Credit Card industry's deceptive advertising targeting children

cartoon of the month

MONDAY, MAY 23, 2005

RBI leaves the field to privateers

Another prime example of how the RBI - Reserve Bank of India continues to shirk their work. The IBA (Indian Banks Association) is the cartel of private and foreign Banks who have the RBI in their pocket as evidenced by RBI's Working Group report on the Credit Card industry in India.

IBA plans firm for centralised clearing system
Our Banking Bureau / Mumbai May 21, 2005 (source: Business Standard website)

Indian Bank's Association (IBA), in association with member banks, will form a company that will act as an umbrella organisation for operating all retail payments and settlement systems in India.

The umbrella organisation will own and operate the clearing system in India. A slew of banks including ICICI Bank, Citibank, Standard Chartered Bank and 12 public sector entities are likely to pick up stake in this company.

At present, there are 1,050 clearing houses in India. In addition to this the RBI had appointed State Bank of India and its associates and 12 public sector banks as its clearing agents.

"The company will act as a holding body and the 1050 clearing houses will act as franchisees," said Reserve Bank of India executive director R B Barman.

"The IBA has conveyed its in principle approval to co-ordinate the formation of this company to the RBI," said Barman.

"The proposed company will be formed by a group of banks based on their participation in the clearing system and the existing 12 PSU banks will also have an equity stake in this

Ex RBI GM K.Vijayraghavan comments

VISITOR FEEDBACK

NAME

E-MAIL

YOUR QUERY

Submit RESET

ARCHIVES

05/16/05
05/17/05
05/18/05
05/19/05
05/20/05
05/21/05
05/22/05
05/23/05
05/24/05
05/26/05
05/27/05
05/28/05
05/31/05
06/01/05
06/02/05
06/04/05
06/07/05
06/08/05
06/09/05

company," said a senior IBA official.

Banks like ICICI Bank, Citibank and Standard Chartered Bank are large participants in the clearing system and could pick up stakes in the company, he added.

"IBA has formed a working group which has representatives from public sector banks, private banks, foreign banks and co-operative banks," said the official.

"The working group will decide on the nature and the model of the company," said the IBA official.

This is following the Reserve Bank of India (RBI) announcement in the annual policy suggesting the need for a new umbrella organisation for retail payments systems.

POSTED BY SUPERFLY AT 3:40 PM 2 COMMENTS

Maharashtra Govt.'s contempt of IT Act 2000

Maharashtra Ordinance takes on India
WITHOUT CONTEMPT

Somasekhar Sundaresan / New Delhi May 23, 2005 (source: Business Standard website)

A month ago, this column spoke about the perils in the capital market due to the Maharashtra government's approach to Stamp Duty legislation. (Stamping out Mumbai's Capital Market in edition dated April 11, 2005).

In keeping with expectations, a few days ago, the IT-savvy governor of Maharashtra promulgated the Bombay Stamp (Amendment) Ordinance, 2005 amending the Bombay Stamp Act, 1958 to provide for stamp duty on electronic records of securities transactions.

Couched in the garb of stamp duty, the Ordinance imposes a transaction tax on securities transactions in violation of the Constitution of India.

The Ordinance also results in extra-territorial taxation of transactions. Securities transactions that have no connection with Maharashtra can now face the incidence of stamp duty.

The Ordinance blatantly attempts to undo the benefits conferred on the securities market by Parliament. **The stated object of the Ordinance is to "to cope with the new form of trading after inception of the Depositories Act, 1996 (Act No.22 of 1996) and the Information Technology Act, 2000 (Act No. 2) of 2000)".**

With the Depositories Act, Parliament had ensured that transactions in dematerialised shares would be free of stamp duty. The Maharashtra government wishes to re-impose this duty through the back-door.

Since stamp duty is not a transaction tax but a duty payable on the creation and execution of specified instruments, the Ordinance has inserted a new Article 51A that imposes an ad

06/10/05
06/11/05
06/18/05
06/20/05
06/24/05
06/29/05
06/30/05
07/01/05
07/05/05
07/08/05
07/09/05
07/11/05
07/27/05
08/11/05
10/04/05
01/12/06
03/17/06
09/16/06
07/16/07

FEEDS

Site Feed
XML

valorem stamp duty payable on every recording of a transaction of a securities or commodity broker, whether in electronic or physical form.

Under the Constitution, taxation of securities transactions is clearly out of the ambit of state legislature and rests squarely within the powers of Parliament, which is why the Depositories Act did away with stamp duty on trading in dematerialised securities. Even the rate of stamp duty on transfer deeds for trading in physical shares may be prescribed only by the central government.

Here is why Article 51A is a transaction tax:

An electronic record of every transaction would be contained in the computer systems of the buying broker, the selling broker, their respective clients, and of course, also in the server of the stock exchange.

Each of these electronic records is an instrument within the charge of Article 51A unless Maharashtra amends the law to clarify which of these instruments recording the same transaction would be amenable to stamp duty. This, in turn, would further underline the fact that Article 51A only intends to tax the underlying transaction instead of an identifiable instrument.

Another important trait of this back-door transaction tax is that the Ordinance imposes a lighter ad valorem duty on speculative day traders who contribute to trading volumes as compared with the duty on transactions that result in delivery identical to the duty structure imposed by Parliament for the securities transaction tax.

If Article 51A is not a transaction tax, any state legislature can impose stamp duty on books of accounts of every person (these will clearly be ‘instruments’) and charge ad valorem stamp duty as a percentage of the profits recorded in the books.

If Article 51A is not a securities transaction tax, such a duty on books of accounts will not be income-tax (on which only Parliament can legislate).

Worse, the Ordinance has extra-territorial implications. If the record of every transaction stored in the servers of stock exchanges headquartered in Maharashtra is an instrument amenable to stamp duty, transactions by brokers who have no presence whatsoever in Maharashtra would also face the incidence of stamp duty.

On the other hand, if records of transactions of outstation brokers are exempted from stamp duty despite the instruments residing in the servers located in Maharashtra, it would further underline the fact that Article 51A is but a transaction tax.

Apart from being unconstitutional, the imposition of yet another transaction tax on securities transactions will lead to volumes drying up. Not many are yet aware of the full implications of the Ordinance. This is a piece of law that cries out for a federal review.

(The author is a partner of JSA, Advocates & Solicitors. Views expressed here are his.)

by: "mailto:somasekhar@jsalaw.com"

POSTED BY SUPERFLY AT 2:29 PM 0 COMMENTS

RBI, of forged notes, fake Banks, police inaction

It seems that you can teach an old dog new tricks after all. Senior Officers of the Reserve Bank of India (RBI) were foxed when SarbaJit Roy's Hacking Complaint confronted them with the fake Bank styled as "Standard Chartered Grindlays Bank" which had operated in India for over 2 years without any Banking licence, and which bogus Bank had also hacked the database containing Credit Card details of over 12 lakh ANZ Credit Card holders in India.

So does this show that after fake Banks, the RBI has no control over its own staff either? Especially if currency notes marked for destruction can find their way into salary packets of Government employees.

National Library files FIR against Canara Bank
Imran Ahmed Siddiqui (source: Indian Express Newsline)

Kolkata, May 21: THE National Library authorities today lodged an FIR against the Canara Bank's Brabourne Road branch after fake notes of Rs 500 denomination were found in the employees' salary.

Eleven such notes, bearing the Reserve Bank of India's ''Forged Note'' stamp, were found in the salary issued to the employees of the National Library and the Archaeological Survey of India.

The salary had come from Canara Bank's Brabourne Road Branch on April 30.

''We have lodged an FIR against the Canara Bank, as they issued the notes of Rs 500 denominations which were already marked as 'Forged' by the Reserve Bank of India (RBI). Those notes were not to be put in circulation. The complaint was lodged by the head office,'' said Saibal Chakraborty, an official of the library.

Asked how it happened, S Chowdhury, chief general manager, RBI, Kolkata, said: ''It is a very serious matter. We have to investigate how it happened. We have given specific instructions to our staff as well as to other banks not to give fake note to customers. But the important question is how these forged notes reached the Canara Bank from the RBI. And why they did not intimate us''.

Meanwhile, the authorities of Canara Bank, Brabourne Road branch, blamed the RBI for the fiasco after the Newsline reported about the detection of the fake notes.

The assistant general manager of Canara Bank, Brabourne Road branch, BN Roy, said: ''We are also at a loss of words as these notes bore the stamps of RBI as ''FORGED'' and still ended up in salary. They are supposed to be destroyed''.

The fake currency racket has even reached the Lalbazar. Newsline reported in March that fake notes of Rs 500 and Rs 1000 denominations were detected in the salary of policemen.

The notes on that occasion had come from the Reserve Bank of India.

Admitting that the fake currency racket is too deep, Chowdhury said: ‘‘we found that fake notes which reached Lalbazar were not issued by the RBI. So there is no question of exchanging them’’.

His statement is at variance with that of the police commissioner, Prasun Mukherjee, who had said that the fake notes were part of the salary which comes every month from the RBI.

Chowdhury said the RBI is planning to provide training to several bank officials in the wake of this spurt in fake currency circulation.

Fate of Fake Currency
The RBI receives fake notes from other banks. These are mechanically tested
The words ‘Forged Notes’ are stamped on the notes
The RBI lodges a complaint with police
The fake notes are kept separately and later destroyed

POSTED BY SUPERFLY AT 2:13 PM 0 COMMENTS

Cyber law and privacy in India

surprising the Times of India missed out on the Supreme Court's "Auto Shankar" judgement

The law isn't much help
SHARVANI PANDIT

TIMES NEWS NETWORK[SATURDAY, JANUARY 15, 2005 08:25:23 PM]

Technology is advancing, voyeurs are getting ever more intrusive, but India's laws are struggling to keep pace. As things stand, if your privacy has been intruded upon and you want to get the offender punished, the law isn't much help.

Cyber law expert and advocate Pawan Duggal points out: "There is legal protection against the Centre and states violating the privacy of an individual, but there is nothing to stop another private individual from doing so."

The Supreme Court first recognised in 1964 that the right to privacy is implicit in the Constitution under Article 21, which specifies the fundamental right to life. But the ruling applies only to the state and falls under the Protection of Human Rights Act, which led to the formation of the national and state human rights commissions. What about the recent wave of hi-tech crimes? Most of these cases would fall under the IT Act, 2000, and the Indecent Representation of Women (Prohibition) Act, 1987, and some sections of the Indian Penal Code. While showing and distributing pornography is illegal, viewing it is not.

The IT Act deals with offences of publishing or transmitting or causing to be published any kind of obscene information. Its ambit extends over information that is lascivious, or which appeals to prurient interests or if the effect is such as to deprave or corrupt persons who are

likely to hear, see or read it. While the IT Act is not gender-sensitive, it is relatively stringent. It overrides inconsistencies due to any other act. The first conviction is punishable with a five-year sentence and a Rs 1-lakh fine; the second 10 years in jail and a Rs 2 lakh fine

Section 292 of the IPC deals with selling or distributing of obscene information like brochures and pamphlets. Conviction could result in three years in prison, while the fine is determined by the judge. There's also the Indecent Representation of Women (Prohibition) Act, which seeks to check this practice in advertisements, publications, writing, painting, figures or any other manner. But the maximum penalty is just two years in prison and a Rs 2,000 fine.

The issue of the right to privacy also raises another question. Should the use of hidden cameras be regulated so that they can be used for 'fair' purposes – like exposes by the media? Duggal says he would support such regulation, but adds that in cases where "the rights of the individual are infringed and unsuspecting individuals are filmed to cater to voyeuristic needs of others, the law should have stringent punishments like five years in prison not just for the cameraman but also the distributor." Senior lawyer Kirti Singh agrees. "The laws need to be made strong enough to ensure such incidents are curbed."

Duggal also stresses the need to train the police. "It is essential that the police be equipped to handle such crimes as they are the first contact with the complainants," he says. **He claims that 500 cyber crimes occurred in Delhi last year, of which only 50 were reported and charges framed in only one case.**

Deputy Commisioner of Police Tajinder Luthra agrees: "Some changes are needed in the IT Act, as under it only ACPs or Deputy SPs can investigate such crimes. This restricts and makes our resources smaller."

POSTED BY SUPERFLY AT 11:59 AM 0 COMMENTS 

Judicial system pummels cyber law enforcement

Judicial system pummels cyber law enforcement
by Sarbajit Roy, 22-May-2005

This is one of my rare original posts. I am motivated to post this commentary since in my humble opinion the higher Judiciary in India is not taking seriously the enforcement of cyber laws in the country. By way of illustration I am posting sequentially all the listed orders from the website of the Delhi High Court in the recent (pending) matter of *"ANTARES SYSTEMS LTD. Vs. C1 INDIA PVT. LTD. & ORS."* where learned Cyber Advocates are battling it out. I have absolutely no opinion /comments on the merits of this case and I am not interested in any way in this matter. It is depressing to know that the Delhi High Court is the appellate court for orders of the Cyber Regulatory Appelate Tribunals (which have still not been constituted even after 5 years of the Information Technology Act becoming law). Is it no wonder then, that ordinary people get discouraged from complaining about cybercrime in India, while the only people who seem to be making money are the

advocates with their delaying tactics.

IN THE HIGH COURT OF DELHI AT NEW DELHI

12.05.2005

Present : Mr.R.B.Singh, proxy counsel for the plaintiff.
Mr.Kamal Nijhawan for defendants No.1,2 and 5.

+ IAs No 8865/03 and 7000-02/03 in CS (OS) No 1357/2003
Counsel for the plaintiff is stated to be out of country. Adjournment prayed.
List again for disposal of IAs on 12th September, 2005.

May 12, 2005 R.C.CHOPRA, J.
rk.

IN THE HIGH COURT OF DELHI AT NEW DELHI

04.03.2005

Present : Ms.Richa Mohan, proxy counsel for the plaintiff.
Mr.Kamal Nijhawan for defendants No.1,2 and 5.

+ IAs No 8865/03 and 7000-02/03 in CS(OS) No 1357/2003
Learned counsel for the plaintiff is not available. Adjournment prayed on personal grounds.
List again for disposal of the IAs on 12th May, 2005 at 2.00 p.m.

March 04, 2005 R.C.CHOPRA, J.
rk

IN THE HIGH COURT OF DELHI AT NEW DELHI

13.01.2005

Present : Mr.Pavan Duggal with Ms.Richa Mohan for the plaintiff.
Mr.Kamal Nijhawan with Ms.Yashmeet for defendants No.1 and 2
Mr.Manoj Saxena, proxy counsel for defendants No.6 and 7.

+ IAs No 8865/03 and 7000-7002/2003 in CS(OS) No 1357/2003
Counsel for defendants No.6 and 7 is stated to be indisposed. Adjournment prayed.
List for disposal of IAs on 4th March, 2005 at 2.00 p.m.

January 13, 2005 R.C.CHOPRA, J.
rk

IN THE HIGH COURT OF DELHI AT NEW DELHI

01.11.2004

Present : Mr.Pawan Duggal and Ms.Richa Mohan for the plaintiff.
Mr.H.L.Tiku,Sr.Adv.with Mr.Kamal Nijhawan, Mr.H.K.Gulati and Ms.Yashmeet for defendants 1and 2.
Mr.Manoj Saxena for defendants no.6 and 7.

+IA 4498/2004 and CS(OS) 1357/2003
On the request of counsel for defendants no.6 and 7, as a last opportunity adjourned to 13th January, 2005.
Interim orders to continue.

November 1, 2004 R.C.JAIN, J.
sp

IN THE HIGH COURT OF DELHI AT NEW DELHI

23.07.2004

Present : Ms.Richa Mohan for the plaintiff.
Mr.Kamal Nijhawan for the defendant.

+IA 4498/2004 in C.S.(OS)No.1357/2003
For the reasons stated in the application, the application is allowed.
Adjourned to 1st November, 2004.

JULY 23, 2004 R.C.JAIN, J.
sp

IN THE HIGH COURT OF DELHI AT NEW DELHI

13.04.2004

Present : Mr.Pawan Duggal for the plaintiff.

No time available today.
List again on 23rd July, 2004 at 12.30 p.m.

April 13, 2004 R.C.CHOPRA, J.
rk

IN THE HIGH COURT OF DELHI AT NEW DELHI

10.02.2004

Present : Mr.Pawan Duggal with Ms.Richa Mohan for the plaintiff.
Mr.S.K.Taneja, Sr.Advocate with Mr.Kamal Nijhawal and Mr.H.K.Gulathi for defendants

No.1 and 2
Mr.Munish Kochhar for defendants No.3 and 4
Mr.T.V.Ratnam with Mr.A.Ranganadhan for defendants No.6 and 7

+ CS (OS) No 1357/2003 and IAs No 8865/03 and 7000-7002/2003
Counsel for the plaintiff prays for adjournment as he is not feeling well.
List again for arguments on 13th April, 2004 at 12.30 p.m.

February 10, 2004 R.C.CHOPRA, J.
rk

IN THE HIGH COURT OF DELHI AT NEW DELHI

15.01.2004

Present : Mr. Pawan Duggal for the plaintiff.
Mr. S.K. Taneja, Senior Advocate with Mr. H.K. Gulathi and
Mr. Manmeet Jarnwal for the defendants No.1 and 2.
Mr. Munish Kochhar for the defendants No.3,4 and 5.
Mr. T.V. Ratnam with Mr. A. Ranganadhan for the
defendants No.6 and 7.

+ CS (OS) No 1357/2003 and IA Nos 8865/2003 and 7000-7002/2003
No time available today.
List again for arguments on 10th February, 2004, at 12.30 P.M.

January 15, 2004 R.C.CHOPRA, J.
vk.

IN THE HIGH COURT OF DELHI AT NEW DELHI

09.12.2003

Present : Mr. Pawan Duggal for the plaintiff.
Mr. H.L. Tikku, Senior Advocate with Mr. Kamal Nijhawan and Mr. H.K. Gulati for the
defendants No.1 and 2.
Mr. Manish Kochhar for the defendants No.3,4 and 5.
Mr. T.V. Ratnam with Mr. Buddy A. Ranganadhan for the
defendants No.6 and 7.

+ Suit No 1357/2003 and IA Nos 8865/2003 and 7000-7002/2003
The Court is busy in some other matters.
List again on 15th January, 2004, at 2.00 P.M.

December 09, 2003 R.C.CHOPRA, J.
vk

IN THE HIGH COURT OF DELHI AT NEW DELHI

23.10.2003

Present : Mr. Pawan Duggal for the plaintiff.
Mr. H.L. Tikku, Senior Advocate with Mr. Kamal Nijhawan and Mr. H.K. Gulathi for the defendants No.1 and 2.
Mr. Manish Kochhar for the defendant No.5.
Mr. T.V. Ratnam and Mr. Buddy A. Ranganadhan for the
defendants No.6 and 7.

Mr. Manish Kochhar, Advocate, has appeared and accepted service on behalf of defendants No.3 and 4 in pursuance of the publication.
Let a complete copy of the paper book be supply to him. Written statement and replies be filed within two weeks.
Copies of the rejoinders be also supplied to the defendants.
List again for disposal of IAs on 9th December, 2003, at 2.00 P.M.

October 23, 2003 R.C.CHOPRA, J.
vk

IN THE HIGH COURT OF DELHI AT NEW DELHI

03.09.2003

Present : Mr.Pawan Duggal for the plaintiff.
Mr.H.L.Tiku, Sr.Advocate with Mr.Kamal Nijhawan and Mr.H.K.Gulathi for defendants No.1 and 2
Mr.Manish Kochhar for defendant No.5
Mr.T.V.Ratnam with Mr.Buddy A.Ranganadhan for defendants No.6 and 7

+ IAs No 8865/03, 7000 to 7002/2003 in Suit No 1357/2003
Defendants No.3 and 4 do not appear to have been served so far. Issue fresh summons and notice to defendants No.3 and 4 for 1st October, 2003 by registered AD post as well as through approved courier.
Defendants No.6 and 7 have filed their written statements and replies. Defendants No.1 and 2 have filed replies to the application under Order 39 Rule 1 and 2 CPC but have not filed their written statements. Let the replies to all the IAs and written stateme
ts be filed within two weeks. Counsel for defendant No.5 submits that he will be adopting the written statement and replies filed by defendants No.1 and 2.
List for disposal of IA No.7000, 7001, 7002/2003 and 8865/2003 on 1st October, 2003 at 2.00 p.m.
In case defendants No. 6 and 7 and defendant No.1 extend their agreement, the same will be subject to further directions to be passed by this Court on injunction application filed by the plaintiff.
Copy Dasti.

September 03, 2003 R.C.CHOPRA, J.

rk

IN THE HIGH COURT OF DELHI AT NEW DELHI

01.09.2003

Present : Mr.Pawan Duggal for the plaintiff/applicant.

+ IA No 8865/2003 in Suit No 1357/2003
Notice to defendant's counsel for 3rd September, 2003.
Dasti as well.

September 01, 2003 R.C.CHOPRA, J.
rk

IN THE HIGH COURT OF DELHI AT NEW DELHI

13.08.2003

Present : Mr.Pawan Duggal for the plaintiff.
Mr.Kamal Nijhawan with Mr.H.K.Gulathi and Ms.Yashmeet for defendants No.1 and 2
Mr.Munish Kochhar for defendant No.5

+ Suit No 1357/2003 and IAs No 7000 and 7001/2003
Hon'ble Judge is not holding the Court today.
Renotify on 3rd September, 2003.

By order

August 13, 2003 Court Master to
rk HMJ R.C.CHOPRA

IN THE HIGH COURT OF DELHI AT NEW DELHI

21.07.2003

Present : Mr. Pawan Duggal for the plaintiff.
Mr. Kamal Nijhawan for the defendant No.1.
Mr. Munish Kochhar for the defendants No.2 to 5.
Mr. T.V. Ratnam with Mr. B.A. Ranganandhan for the
defendants No.6 and 7.

+ Suit No 1357/2003 and IA Nos 7000 and 7001/2003
Defendants No.3 and 4 have not been served. Issue dasti summons/notices on fresh address of defendants No.3 and 4.
Written statements and replies be filed within a week. Replications and rejoinders, if any, be

filed within a week thereafter.
List for disposal of I.A. Nos.7000/2003 and 7001/2003 on 13th August, 2003.

July 21, 2003 R.C.CHOPRA, J.
vk

POSTED BY SUPERFLY AT 11:10 AM 0 COMMENTS 

Asian School of Cyber Laws, Pune (ASCL)

I came across this article today at the ASCL Cyber Laws website, several posts today are based on articles from this Asian Cyber Crimes Law School site. This particular article has prompted me to add my extensive in-line comments. Interested readers are advised to read my HACKING COMPLAINT and associated rejoinders after perusing this article and my comments.

Banking Frontiers September, 2002

by Rohas Nagpal, Asian School of Cyber Laws

MYTH 1 – "Email messages are confidential can be trusted".

In a world where email spoofing is literally becoming child's play this statement is no longer a myth – it is a lie. In the past email spoofing, where an email appears to be sent by someone but has actually been sent by some other person, has brought many to financial ruin.

Take the case of an Indian bank which recently faced a run because email, supposedly sent by its manager, informed customers that the bank was facing financial troubles. In another case, a Pune based businessman was conned out of Rs 10 lakhs by a Nigerian who was pretending to be the Vice President of the African Development Bank. The businessman trusted the senders email address as was showing in the email that he received.

The only way to protect yourself is to digitally sign and encrypt all email messages.

YEAH, except that it costs Rs.25,000 to obtain a digital signature with umpteen hassles and paperwork every year. PLUS every computer in every Bank branch will need a unique digital signature => loads of revenue for the government.

MYTH 2 – "We have firewalls installed. We are totally safe."

Untrue. In reality almost all firewalls, in the past, have been broken into. Bugs have been discovered in some of the best firewalls in the world. A new version is introduced as soon as the bugs in the earlier version become public. Then a newer version is introduced as soon as the bugs in the earlier version become public and so on…

Instead of trying to secure your position by installing criminally expensive firewalls, prefer

using Virtual Private Networks based on Public Key Infrastructure.

So what if VPNs are illegal in India, and that DoT only allows maximum 40 bit encryption ?

MYTH 3 – "We are using the best antivirus. There's no way we can get infected".

Now let us face the facts. Suppose your company buys the latest anti-virus package. The anti-virus company provides you with regular updates. So, you update once a month. Each day 30-50 new viruses are created and released into 'the wild". What if you get infected between upgrades? Anti-viruses, and by this we mean all anti viruses work on a reactive basis. So first the virus attacks then the patch is made. No anti-virus anticipates the new viruses it will have to face.

To drive home the point, consider that case of the idiot virus. This virus would scan all your communication and wherever it found the words Sir or Madam it would change them to IDIOT. Imagine bank statements going out to thousand of customers that start with the words "Dear Idiot,"!

Another virus, the ILOVEYOU virus, enjoys the distinction of having been the most prevalent virus in the world. This virus was created in the Visual Basic language. Losses incurred due to this virus were pegged at US $ 10 billion! The virus used the addresses in the victim's Microsoft Outlook and e-mailed itself to those addresses. The email, which was sent out had "ILOVEYOU" in its subject line. The attached file was named "LOVE-LETTER-FOR-YOU.TXT.vbs". people wary of opening email attachments were conquered by the subject line and those who had some knowledge of viruses, did not notice the tiny .vbs extension and believed the file to be a text file. The message in the email was "kindly check the attached LOVELETTER coming from me". this virus first selected certain files and then inserts its own code in lieu of the original data contained in the file. This way it creates ever-increasing copies of itself.

The 5% virus – that is what the original version was called. This virus affected mainly financial institutions. Its effect was tht it would take all the figures in your computers and alter them by either increasing or decreasing them by 5%. Later versions changed the percentage of alteration to 1.35 or 2.7% making it even more difficult to trace the alterations.

The solution. Do not blindly trust any anti-virus package. Set down inviolable rules about email attachments – whether they may be opened from office computers or not. No computer that has even remotely important data on it should have any connectivity to the Internet. If this computer is on a network the entire network should have no connection whatsoever with the Internet Employees should not be allowed to use their floppies on office computers.

Read my Hacking Complaint and weep to discover that the RBI ONLY permits Banking data to be transferred over floppy disks (??) entered by Bank Employees for their sensitive Electronic Clearing Systems and all Electronic Fund Transfers.

MYTH 4 – "If something is password protected, I bet it cannot be broken into."

If you make this bet, you'd feel sorry. Most passwords are short and very simple to crack. To

stop it most passwords are based on common names, birth dates, telephone numbers etc. these are, of course, the first passwords that any hacker will try. It's easy enough to crack passwords; such users just make the hacker's job easier.

The hacker could actually pretend that they are really close to you till you trust them. And obviously, since they are from the rusted gang you wouldn't think twice about "mistakenly" telling them your password. Why would they possibly want to harm you, right? Then there are those who are experienced in the use of computers but can't always remember their password. So, what do they do? They put these passwords on POST-IT notes and stick them on their monitors thinking, "No one would really think of looking for passwords there, would they?"

Even if you do not make any of these bloopers, all a hacker would need to break your passwords, is a good password cracker. Just a small piece of trivia – the good crackers are quite capable of checking 75 lakh passwords per second! The best way to avoid such ugly situations….keep long alphanumeric symbolic machine generated passwords (like a_7834ee*A98Y!$%), change passwords frequently and have a well defined organizational password policy.

Ho, Ho Ho, Infosys's Finacle Software ran at numerous branches of the Bank of India, and the default system password for many years was "SAFALTA" - BOI's slogan- and the employees either COULDN'T or WOULDN'T change this password.

MYTH 5 – "Operating systems have built in dependable security features"

That one is a joke. It is common knowledge that most operating systems (OS) will provide only a very basic level of security against breaches. If that's what you are depending on, you might as well present all your critical data to the attackers on a CD ROM. The solution? Do NOT trust only your OS. Use a combination of electronic and information security techniques for data protection.

Is this infantile "Myth" even worth replying to?

MYTH 6 – "Once a month, we backup all our data on another drive."

Big Mistake. Most institutions take regular backups onto another drive. What happens if a virus infects the computer on which regular backups are taken and all the files are destroyed? Backups should be taken in real-time, and additionally stored on removable media like CD-ROMs.

GREAT - Rohas would prefer that we backup storage of sensitive Banking information over the Internet? One of my grievances in the Hacking Complaint was that Standard Chartered Bank was storing all their Credit Card information for Indian Credit Card Holders in Malaysia. During the Hearings SCB lawyers refused to disclose where they are storing and maintaining sensitive Banking data on Indian credit card accounts and also where they were backing up their credit card information and also the mandatory information security measures they take. The RBI has f***ed SCB royally after I highlighted this.

MYTH 7 – "Since banks use it, banking software is absolutely bug-free."

No software is completely bug-free. Time and again hackers have proven this fact much to

the chagrin of the banks. The best banking software have been shown to have major flaws. In many cases the software developers deliberately leave flaws or backdoors in the software. And you have to consider the fact these are finally human. They can make mistakes. These vulnerabilities are later exploited to commit huge frauds. This one has no perfect tailor-made solutions. Choose a proven software solution and … pray.

SAFALTA at long last

MYTH 8 – "Anyways, if something goes wrong, our team of experts can handle it."

Wrong. If a security breach occurs, brings in the experts. Do not try to investigate in house. You may end up doing irretrievable damage with nothing to show for it. Electronic evidence is inherently volatile and will disappear if you try to investigate without expert assistance. A team of the FBI's (USA) topnotch cyber crime investigators raided the premises of a suspect and confiscated his computers. Keep in mind that these guys were some of the best in the world. When they reached their labs and reconnected the computers they found that there was nothing on them.

It was later found that the suspect had put extremely powerful magnetic coils around his door. When the computers were taken through that door, all the data on them was completely deleted and erased!!

When my Bank's PC hangs they have to wait for the guy with the AMC contract to walk in and take out the PC with this sensitive information to their "lab" where they can "dissect" the innards at leisure.

MYTH 9 – "OK. If a breach occurs, we will wait for the experts to come in before doing anything?

Wrong again. All your employees should be trained in basic emergency response. A security breach should not create FUD (Fear, Uncertainty or Doubt). All employees should know that panic would not help. They should be well aware of the countermeasures, which will need to be taken. These basic countermeasures are of course dependent upon the systems and software in use.

A bank in London was hacked into. Their intrusion detection system (IDS) immediately alerted them to the breach. The authorities of the bank called in a team of experts for investigation. This team arrivged one and a half hours later. By then the attacker had stolen tons of customer account information and erased most of the evidence. The Computer Emergency Respoonse Team (CERT) later said that had the bank employees disconnected the target computer from the network, 90% of the data could have been saved.

Whenever I see my Bankers (a nationalised Bank) I doubt very much if they even know what their systems and software are, leave alone the counter-measures to be taken. The second para fully justifies why are Indian Commies (CPI-M) are absolutely correct when they want to ban automation in the Banking sector.

MYTH 10 – "What's the point in trying to report anything to the police? They can't do anything anyway!"

This is one of the most blatant statements of ignorance. Many police departments today are well trained to handle cyber crimes and are aware of the legal provisions. Make sure that the local police are informed as soon as any breach is detected or suspected. If the collection of evidence is not done meticulously and as per the law, the criminals will walk free.

THIS IS THE BIGGEST CANARD OF THEM ALL. Run away from the Police as fast as you can. When I went to my local police thana initially to register my Hacking Complaint, the SHO told me "Sa'ab for me and my Investigation Officers IT ACT means Immoral Trafficking (in Women) Act, and me and my boys don't even have a PC and since we don't have a copy of your(!) IT ACT we can't register the FIR." Incidentally FIRs can only be registered by the SHO of Police Station, and going to the Cyber Cells of Police are an exercise in futility and corruption, because the cops there will contact the other side - take money - and then register an absolutely diluted FIR at some pliable police station - as it seems happened in the DPS:MMS-Baazee.com case.

POSTED BY SUPERFLY AT 9:44 AM 1 COMMENTS 

Information Technology Act 2000 myths

Is it any wonder that Cyber Crime in India is exploding if the national press publishes ill informed stories like this? Secondly what is the quality of courses and faculty at the Asian School of Cyber Laws if they publicise this kind of garbage and mis-information?

(source: Zahra Khan Times News Network)

Beware what you access on your computer. The cyber police is on the prowl.

Did you know that creating an e-mail account on a false name is illegal? Did you also know that forwarding pornographic pictures to your friends over the internet makes you criminally liable? And that you could be fines crores of rupees in addition to jail time for such ‘crimes’?

Every day, millions of people use the internet to send and receive e-mails, download files and surf websites looking for information or gratification among other things. Every little thing that we do the internet is stored in our computer’s hard disk and can be traced back to us if need be.

After the IT revolution came the inevitable cyber crimes. What followed was the IT Act 2000. as per the Act, any “unlawful acts wherein the computer is used, either as a tool or a target or both” is termed as a ‘cyber crime’.

Imagine forwarding a humorous e-mail attachment to a few of your friends. The next thing you know you’ve been accused of sending an e-mail virus through the attachment. Even sending a virus unknowingly or accidentally can make you liable for up to rupees four crore as fine. And of course, the jail time for three years, if you get convicted. But this is only Section 43 (c) of the Act.

Section 67 of the IT Act is the most serious legislative measure against pornography. Offences of ‘publishing, transmitting or causing to be published, pornographic material in

electronic form' are registered under this section. If you send or forward anything even remotely pornographic in content, it becomes a case of unauthorized electronic publishing, and the Act prescribes imprisonment of up to five years plus rupees one lakh as fine, if the case is a first conviction.

Shuchi Nagpal, the Information Officer at the Asian School of Cyber Laws explains,"the reason why cyber crimes attract greater criminal liability as compared to regular criminal cases, is because the extent of damage is far reaching. Take the case of cyber pornography for instance. Pornographic distribution is not that much through magazines, but over the internet. In order to achieve stricter implementation of cyber rules and to curb illegal activities on the internet, such stringent laws with serious consequences have been enforced."

'Hacking' or the unauthorized access of computer systems and networks is covered by Section 66. it provides for imprisonment of up to three years and a fine of rupees two lakh as penalization. Nowadays, almost all companies have employees logging onto systems with a unique username and password. If someone misuses your identity on the network, then you become liable, whether it was you who committed the crime or not.

Another activity that could get you in a lot of trouble is posting on internet message boards and bulletins. If you happen to be in an internet discussion group or forum and post some remarks or personal opinions, especially against the Government or the Constitution of India, you become criminally liable and can be sentenced to life imprisonment if convicted!

A big misconception among the masses is that such crimes cannot be traced. On the contrary, tracking emails is very simple. Each time you log on to the internet, you are allotted an IP address which is very easy to trace within a matter of minutes and in some cases hours. But nevertheless, it can be tracked. Another method of tracking down an email is to view the header – all you need to do is the press 'Options' button in your e-mail program and go to 'Preferences'.

This will throw up two boxes where you can view the origin of the e-mail in full detail, including the IP address.

So every time you log on to the internet, be careful what you do. For all you know you might have the men in khaki knocking at your door, and of course your PC!

Do you know your cyber laws?

* Section 43 (c) - sending a virus - Rs four crore fine, three years jail
* Section 67 – forwarding pornographic material - Rs one lakh fine, five years jail
* Section 66 – Hacking into accounts - Rs two lakh fine, three years jail
* Posting remarks against the Government or Constitution – life imprisonment

POSTED BY SUPERFLY AT 9:37 AM 0 COMMENTS 

IT Minister's digital signature hacked

(Source: The Hindu Business Line)

The digital signature is here to stay but must be tested for efficacy to suit the Indian context. The more secure a prison, the greater the thrill in breaking it. The spirit of the erstwhile Alcatraz is testimony to this.

This seems to apply to digital signatures now in cyber world. The passage of the Information Technology Act on October 17, 2000, legalised digital signatures in India. Various standards and infrastructures involving cryptography have also been put in place. This signature is intended to be unique to the individual and to serve as a means to identify, authorize and validate. But if so important a signature can be misused or misrepresented, is it not time to take notice?

The debut of digital signatures in India was in February this year when the Prime Minister received a digital e-mail from Pramod Mahajan, the Minister of Information Technology. According to the mail received, the digital signature was assured to be that of Mahajan.

A digital signature is used to authenticate the identity of the person who sends an electronic message. With the use of digital signatures, electronic transactions on the Internet can have a legal standing. So, the promise of the paperless revolution is still a possibility.

But the Indian Government does not seem to be too keen on digital signatures. Otherwise, when the controversy on the use of the MD5 (message digest 5) hash function and the SHA 1 hash function came to light, the Government should have been the first to ensure that it did not go through.

The MD5 hash function, which was brought out by RSA Inc of the US, has been found to be breakable which has been testified by the company itself way back in 1996. According to CryptoBytes, a technical newsletter of the RSA Data Security Inc, hash functions are frequently used cryptographic primitives and in digital signature schemes, a message is hashed before signing.

This signature should be collision-resistant in the sense that there should not be another hash function, which is similar in nature but has a totally different meaning to it.

According to the journal, it was found that this MD5 hash function could be broken and at that point of time, "we suggest that in the future MD5 should no longer be implemented in applications such as signature schemes, where a collision-resistant hash function is required."

Digital signatures are the only practical solution for electronic communication. A digital signature by nature is such that it binds the signatory, the signature and the message. Tampering with the original message can be immediately detected if the message has been digitally signed. This leaves very little scope for forging a signature, Nagpal says.

To get your digital signature, you first need to apply to a certifying authority (CA). The company will then allocate a private key and a public key to you. These "keys" are mathematically related and are used to encrypt and decrypt your digitally-signed documents. This procedure is referred to as public key cryptography. You use your private key to "digitally sign" or encrypt a message and at the other end the recipient who already has your

public key uses it to decrypt your message. Two things are essential - as the name suggests, only you and the public key to the recipient should know the private key.

"The MD5 hash function, which has been prescribed by Indian law, has been globally recognized as being insecure for use in digital signatures. In light of this, the decision to prescribe the MD5 hash function for use by the Certifying Authority in India is erroneous and could have serious repercussions for the proposed Public Key Infrastructure in India. It would also imperil national security," says Nagpal.

Additionally the police departments are gearing to accept digitally-signed complaints online. "If there is discrepancy in the law, just think of the number of disputes that it would throw up. As it is we are under pressure to resolve litigation. This kind of a problem will only result in more work for us," police officials say.

Online banking transactions are gaining ground in India and in future these will use digital signatures.

What are the other areas where digital signatures can be used? Contracts, Government communications (e-governance), Defence organizations and law enforcement. Digital signatures are used to authenticate any kind of electronic communication.

The present attack does not yet threaten the practical applications of MD5, but it comes rather close to it. It appears to be the right time to look at the implications of such a problem rather than just seek to blindly apply technology.

POSTED BY SUPERFLY AT 9:33 AM 2 COMMENTS