PRSENSE

Communicate the communication

India's first Corporate ezine

Issue No 32 – Oct 2008

Published by Prime Point Foundation

Theme of this issue

Cyber crime

Guest Editor

Mr N Vittal

N. Vittal IAS (Retd)
Former Central Vigilance Commissioner of India

In this Issue:

Contact

www.corpezine.com

editor@corpezine.com

PR-e-FACE: From the desk of Editor in Chief

"Fight the cyber challenges and make the cyber space risk free"

Presently, technology is growing at lightening speed. While the technology brings lot of good things, it also brings equal amount of risks and challenges. Every day, we read in the newspapers about the various cyber crimes, like Credit card cloning, spoofing, phishing, stalking, etc. Some of the youngsters indulge in misusing the technology and get caught by the Police Authorities.

A recent study revealed that 80 percent of the cyber crimes in the Corporate Houses are committed by the 'insiders'. More than 95 percent of the cases do not get reported to the Police Authorities.

Many Governments across the world have enacted laws to deal with the cyber crimes sternly. Awareness about the cyber risks are yet to percolate amongst the Corporate Houses and also individual internet users. Many of the well known corporates also do not have proper 'cyber security' in place. 'Cyber espionage' is a great challenge for many business houses in the world. 'Cyber terrorism' is another challenge facing the humanity. We should not wake up only when the damages happen. There is an urgent need for creating awareness about the cyber risks.

In this issue, we are trying to bring out the fundamental awareness about the cyber crimes and various types of risks that we are facing. Wherever possible, we have also given few preventive suggestions. We appeal to all the Corporates that they take this development seriously and start debating within their own Organisation.

We are greatly honoured to have Mr N Vittal, Former Central Vigilance Commissioner (CVC) of India as our Guest Editor. During his tenure as Information Technology Secretary and subsequently as CVC, he has sown the seeds of technological development in India. His editorial is a great eye opener for all.

Let us all together fight the common challenges and make our cyber space 'risk free'.

K. Srinivasan

Guest Editor – Mr N Vittal

Mr N. Vittal IAS (Retd) is a well known bureaucrat of Indian Government. He retired as the Central Vigilance Commissioner of India. During his tenure as CVC of India and earlier as IT Secretary to Indian Government, he has made great efforts in developing technology in India. Please listen to his speech on cyber crime

http://www.poduniversal.com/2008/10/cyber-crimes-protecting-your-computers.html

PR-e-FACE: From the desk of Guest Editor

"Human dimension is important in tackling cyber crimes "

For every upside of technology, there is a downside also. Earlier we had the problem of crimes in the physical world and now the same could be done in the cyber world. The added disadvantage is that crimes can be completely committed across borders and they can be committed at the lightening speed. For every productive measure which is taken against the cyber crime, the criminal mind comes out with a cleverer device and discover new loop holes.

These cyber crimes can be tackled on three broad categories. First one is the 'human dimension'. Ultimately, it is the greed of the humans and the cleverness which gives temptation for committing crimes in this sector. You can therefore, look upon the whole issue of tackling the cyber crime from a HR dimension. While attracting and retaining the talent is necessary, the challenge is to see how the best brains are not only retained but also make them loyal. The second dimension, is purely technical. Due to the explosive growth of technology, many options are available. For every new type of technical exploitation, solutions can be found. The third dimension, is the judicial dimension. We need to look at the extent to which these crimes can be detected and punished in a court of law, as these crimes are transnational. There is an urgent need for evolving greater international cooperation and evolving common approaches in the legal side. Hence a three pronged approach focusing on the human, technical and the legal aspects is needed for evolving continuous solutions. The information technology has brought the expression 24 x 7 as a common use. There is no relaxation or holiday for committing crime. Tackling crime on the cyber front also should be a 24 x 7 operation.

I look at the issue of cyber crime in the BFSI section in two different dimensions. The first of course is the utilisation of the information technology for committing crime in the real world. The second one, is the crime that is possible and that takes place only in the cyber space itself. Apart from the individual greed oriented type of crimes, we can also see the emergence of new type of crime which is only peculiar to information technology. This is the crime committed by the intelligent people and it poses an intellectual challenge.

But in recent times, there is another dimension of the cyber crime in the real world what is known as 'Cyber Terrorism'. Some time back the Economist came with a report of how the cyber space is exclusively utilised by the terrorist groups for networking and also for exchanging information. In the BFSI sector, the links to terrorism were obvious from the fact that the terrorists involved in '9/11 attack' were funded using Hawala techniques. The cyber space is becoming very convenient for committing financial crimes. The financial crimes linked to terrorism represent the more important form of cyber crime and special attention needs to be given. The solution to all these problems lies in the technology itself, because of the special nature of the cyber space. I am reminded of the two names of Lord Vishnu in the Vishnu Sahasranama – Bhaya krutha, Bhaya Nashanaha. God creates fear and he also destroys fear. The story of the churning of the milk ocean in Indian Epics also repeats the eternal message. When one wants to get nectar from the churning, initially he gets poison. Unless the poison is controlled one can not get the full benefit of the nectar – amrutha. The same logic also applies to technology tools.

PR-exclusive

"Corporate cyber espionage is a great threat to corporates "

For the last two decades corporate had to protect against opponents using espionage on them to steal confidential information, using variety of means like paying up, making friends to get garbage of their competitors and reconstructing information, getting hold of order copies, invoices, database using all possible means.

Now the corporate espionage has taken a new dimension with usage of computers. The competitors' agents no more break into offices at mid-night. The entire espionage has become centered around the computer system of competitors. There are insider attack on local network and external corporate espionage from cyber space.

Competitors hire a private intelligence organisation or black hat hackers (who hack illegally for money) directly and tell them what information of competitor they want. The black hat hacker goes about identifying the assets of the company (reading more about company, looking at website, writing mails to competitor organisation and finding out who may have the required information. If he knows exactly who owns the information (from his employer) he directly goes behind the information holder.

Once the target is identified, it is kind of easy for black hat hacker. The fundamental of most of these attacks follow the same modus operandi, target stores most confidential information on their machine or laptop and never on central location in corporate. He sends an email to the target like his friend (and tries to deploy a Trojan- data stealing program) once he deploys a Trojan he can get access to the files on target laptop. This technique is called '*social engineering*'.

The next technique could be the black hat hacker talking to the target over a chat; he sends weblink to the target; the target clicks on the link to read up an interesting story, the Trojan - data stealing program gets downloaded to target computer. The target is compromised and the black hat hacker can download any information from target computer.

In the third technique attack can arrive through a pdf file, doc file, xls file. The Trojan - data stealing program is embedded into MS office files or pdf file. If the target machine is not patched for MS office and PDF vulnerability (most computers are patched with latest updates for antivirus, Operating system only). The Trojan could get downloaded from the pdf or doc file and get installed on the target machine.

Central firewall, IDS and two factor authentications cannot help against any of these attacks. Black hat hackers go behind the easy target to gather information using client side vulnerability on the target.

J Prasanna, CEO, AVS Labs, Antivirus & Security Labs jprasanna2006@gmail.com

PRince

BY - TRIAMBAK SHARMA

www.cartoonwatchindia.com
cartoonwatch@gmail.com

SO NEXT TIME PROPOSE HER THROUGH YOUR BLOG... & GIVE HER YOUR BLOG ADDRESS... ITS SAFE FROM "SLAP"

PR-exclusive

"Bloggers: Beware and Be Aware!"

The advantages of the Blog indicates the risks associated with blogging. Being the publisher himself, the blogger has no second person who can unemotionally filter the writing. The writer himself has no time to cool down since his thoughts will fly off and get published even when he is charged with emotions.

There is therefore a need to reflect on how to make positive use of Blogging while avoiding its weaknesses. In this context, there is a need for reflecting on some of the recent bitter experiences of some of the bloggers.

A blogger in Mumbai some time back wrote an article in his blog which was critical of an organization. Unfortunately the organization filed a defamation case against him claiming a damage of Rs 20 million and also brought influence on his employer so that the blogger was forced to resign his lucrative job.

In another incident, an anonymous comment in a blog gave a hyperlink to an obscene file on the Internet. Before Police could lock up the blogger for "publishing obscene information in electronic form" which is an offence which carries an imprisonment of 5 years under Section 67 of ITA 2000, the alert blogger moderated the post and removed the offensive portions of his blog.

These two incidents reflect the impact of Information Technology Act 2000 (ITA 2000) on blogging. After October 17, 2000 ITA 2000 has imposed some responsibilities for all users of IT including bloggers. If one wants to be a blogger, he needs to understand what these responsibilities are and what the consequences of ignoring the legal provisions are.

The law in India provides recognition of electronic documents as equivalent to paper documents and hence whatever expressions are made on the blog is like writing on paper. If it is defamatory or carries any threatening words, it can be considered an offence under the Indian Penal Code (IPC). If it is obscene, it would be an offence either under Section 67 of ITA 2000 itself or under IPC.

There is what is known as the concept of "Vicarious Liability" under which the blog space owner would be held liable for the actions of the visitors who post illegal information. To avoid such "Vicarious Liability" it would be necessary for the blogger to exercise what the law describes as "Due Diligence", which is nothing but adequate precautions that any blogger needs to take to prevent his blog being used for any illegal activities. These principles apply not only to text blogs. It applies to Podcasts and webcasts as well as SMS and MMS. It applies to your You Tube postings, or other postings in message forums or social networking sites.

Na. Vijayshankar, Director, Cyber Law College, Bangaloru (For a more detailed discussion on Legal issues in Blogging, download the free e-Book "Bloggers Beware" from www.naavi.org)

Protecting from Cyber espionage

Most information is stored on laptops or desktop of users. Users are paranoid of storing information in the central server. Central server in any corporate is more secure than rest of location. Users can encrypt data and store on the company server, so that no one will have access to their information (with encryption key no one can access these data).

Use the latest antivirus and personal firewall on their laptops. Store the data on a removable hard disk or an encrypted volume (dont attach or mount it until you need the information), Use keyscrambler to defeat keylogger on your laptop

Corporate should have well configured firewall, Intrusion prevention system. It is always better corporate hire a white hat hacker (good hacker who protects people) to cross check the configuration of network level firewall. Most corporate protect their perimeter and their server effectively, but dont protect end user much (including the CEO, CFO, CIO laptops). These are the places where sensitive information is usually stored. The end user machine will usually be protected by Antivirus and Firewall which is not sufficient to prevent a cyber espionage attack.

By J Prasanna - jprasanna2006@gmail.com

Safe Blogging – Few Tips

1. Avoid using the blog to defame any person.
2. If you feel strongly critical of any issue, restrict your comments to the issue and not on the person. For example, you can say that the "suggestion" made by somebody "is stupid" but not state that the person is himself "stupid".
3. Avoid any "Obscene" information to be posted on your blog. Remember that what is not "obscene" in your view may be so in some body else's view.
4. Use the language with responsibility. Ensure that you use words which are not "accusing" even if they are "expressing suspicion". If possible, refer to other sources causing the suspicion. Let it not be "baseless".
5. Never leave the blog unmoderated. Ensure that only identified persons are allowed to post comments on the blog.
6. If you have made a mistake, don't hesitate to pull down the comment or correct it. Apologize if required.
7. When you reproduce work from some where else, avoid plagiarism and copyright infringement by providing the source details and keeping the reproduction to the minimum necessary. Where felt necessary seek the permission of the source.

- by Naavi – www.naavi.org

Know about ISO 27001

ISO/IEC 27001 is an International standard for Information Security Management System (ISMS). It has 133 security controls spread over 11 security domains. Risk management is the core theme of the standard and it advises organizations to adopt Plan-Do-Check-Act (PDCA) approach to prevent, detect and correct information security risks. Some of the important domains are Security policy, Asset management, Physical security, HR security, Communications security, Incident management, Business continuity management and Compliance. Cyber security is predominant as most of the controls are related to IT environment. Organizations can get certified against this standard. Worldwide about 4800 organizations are certified with Japan first (2700+ certificates) and India stands second with 420+ certificates.

- By M.L.Srinivasan, CEO, ChennaiNet, mls@chennainet.in

What are the Cyber crimes?
- V. Rajendran, Secretary, Cyber Society of India

Phishing: The process by which some one obtains private information through deceptive means, authenticating credentials, in order to assume some one else's identity. The phisher, viz person doing the act of phishing sends an email and leads the victim to some fake web-sites (which appear to be genuine like your favourite bank's web site) and advises the user to divulge his user-id for internet banking along with other private information like password, credit card number and possibly the 3-digit code number in the credit card (called the CVV or the CVC). With such information the phisher then accesses the actual web-site and does an e-commerce or e-banking activity at the cost of the victim.

Skimming is a process of copying the magnetic strip information from a credit card into a small handheld electronic device, called skimmer (now available in the form of contact less and remote facility too) which scans and stores the card data from the magnetic strip. Such information is then passed on to people engaged in the manufacture of counterfeit cards. With the name of the bank and the card-holder (already available at the shop, where the skimming was made) this information will then be embossed in the card and the card looks like original! Fraudsters then indulge in shopping (either personal or on-line) with such fake cards. The victim will come to know of it only after he receives the card statement from the bank.

Computer hacking is the act of getting into some one else's computer involving some degree of infringement on his privacy and causing damage to the information stored therein like computer files or any software. Unlike most computer crimes and computer misuse which are clear cut in terms of actions and legalities like software piracy etc, hacking is a little more complex to define and describe as an offence. Hacking may result in simple invasion or annoyance to a computer or to the point of illegal destruction or otherwise affecting the information therein. Ethical hacking (which is now being taught and learnt as a subject) involves the use of technical knowledge by individuals willing to take the risks required to become a true "hacker" to explore the weaknesses in any system to confirm that the computer system is really robust enough to withstand any hacking attempt.

What are the cyber crimes?

- V. Rajendran, Secretary, Cyber Society of India

Spoofing means maliciously deceiving someone. IP Spoofing refers to the sending data with a forged (spoofed) source Internet Protocol address with the purpose of concealing the identity of the sender or impersonating another computer system and thereby duping the receiver to falsely believe that the mail has been sent by the system whose IP address has been forged. Similarly email spoofing refers to the act of sending an email to make it appear as if it came from somewhere or some one other than the actual one by altering the header information after connecting to the mail server.

Cyber Stalking means causing harassment to someone through computer. Commonly reported forms of stalking include sending repeated emails or SMS to a victim causing mental disturbance or mental agony affecting the behaviour of the victim in a psychological manner. Like receiving obnoxious and objectionable telephone calls, the victim receives emails and SMS from the fraudsters thereby causing embarrassment impacting his mental health.

Key-logger is a software which keeps a log of all the key-strokes, recording the information typed by the user. If a PC has this key-logger software hidden in it and if the user types his user-name and password for an e-commerce or an e-banking transaction, the user information including the password typed by the user can be retrieved from the system (even after he completely logs out). With such gross exposure of the victim's confidential data, his entire bank account including the credit card details and the PIN, e-banking user-id, password are all revealed in the system for use by its owner. This is a grave risk especially when you do an internet banking transaction from a public place like cyber café or a browsing centre.

- By V. Rajendran venkrajen@yahoo.com

Dos and Donts to avoid falling victim of a cyber fraud:

- Never reveal your user-name and password through any email or SMS.
- No bank will ever solicit any personal information through email or an SMS.
- Always look for the site name clearly and ensure the web-site spelling is correct.
- Ensure that the browser display is correct including display of a lock symbol, before making an on-line payment for any transaction.
- Avoid doing e-banking from untrusted and common public place.
- If situation warrants you to do so, ensure that the PIN is changed at the next earliest opportunity.
- Never write the PIN anywhere especially in the hand-bag or the purse.

Resource Centre for Cyber Forensics

Cyber forensics can be defined as the process of extracting information and data from computer storage media and guaranteeing its accuracy and reliability. The challenge is actually finding this data, collecting it, preserving it, and presenting it in a manner acceptable in a court of law. Centre for Development of Advanced Computing, (C-DAC), a Government of India organisation, has developed forensic software to help Police officials involved in investigating cyber crimes. Please listen to the podcast of Mr S Ramakrishnan, Director General of C-DAC. Please click the link

http://www.poduniversal.com/2008/10/c-dac-centre-for-development-of.html

For a safe card transaction, follow the 'card'inal principles:

- Keep the credit/debit card in your safe custody.
- Memorise the CVC or the CVV and then smudge the same in the card.
- Avoid talking to strangers in an ATM.
- Do not take the help of any stranger in an ATM.
- Never part with the ATM card even to the bank staff. If required to do so, handover the card against an acknowledgement noting the time and date.
- Never leave your credit card or the debit card out of your sight.
- If the attendant in any merchant establishment takes the card away from your sight for swiping it in a device, follow him until he swipes.
- Ensure the card is swiped only once and that too only in the authorised device.
- Never leave your credit card or debit card with any one even for a few seconds.
- Leaving your credit card to any stranger even for a few seconds is quite risky, since the stranger may memorise your card number, expiry date and the CVC or CVV which are just enough information for doing an e-commerce transaction like an online purchase of goods, air tickets or rail tickets.

Health Tips

"Tips to fight Jet lag "

Live on a schedule - Weeks or at least days before you leave, you should be maintaining a sensible schedule. People who have no order in their lives, who stay up late to watch a movie and start doing their laundry at 2:00 a.m. have more trouble with Jet lags. Make sure your circadian rhythms (body clock cycles) are in sync.

Set your watch to the new destination time – Start acclaiming yourself to the time change, stay mentally active in the half hour immediately preceding breakfast time at your destination.

Get enough sleep – Shortchange yourself on sleep before your trip and you can just about count on making jet lag worse. Give yourself about 15 extra mins of sleep each of the last few nights before you travel.

Fly by day, arrive at night – The best plan is to arrive at your destination in midevening, get something light to eat, and go to bed by 11:00 PM destination time. This scenario gives your body optimal opportunity to adjust to the change in time zones.

Drink plenty of fluids during the flight – Airplane cabins are notoriously dry and fluids will help combat dehydration. Being dehydrated obviously wont help you beat jet lag.**Avoid Alcohol –** Ask for juice instead. Alcohol is a diuretic and will further dehydrate you.

Be quiet and relax – Use the flight as an opportunity to enjoy solitude and get some relaxation. That way you aren't overstressed before asking your body to suddenly shift 3 hrs.

Do as the romans do – When you arrive, start adapting to your new environment as quickly as possible. Get involved, notice the new street names and the language of the people. This will help you to adjust.

Don't nap – Or if you do, limit the nap to 1 hour. Napping will just delay your adjustment to the new time zone.

Soak up some sunshine – Get out in the sun at your destination as much as possible. This exposure will help keep your biological clock in the stimulated and awake state during daylight hours at your destination.

Think before you react – Put off all important decision making for 24 hrs or at least until you feel well rested. You will not be doing your clearest thinking after a long trip. People have made bad deals and later identified jet lag as the reason.

Reverse the process – If possible, use these tips to prepare for our return flight home too. Jet lag is a two way sky.

Source – The Doctors book of Home Remedies

PR eTTY - Posting of defamatory and annoying messages

The Case of Suhash Katti is notable for the fact that the conviction was achieved successfully within a relatively quick time of 7 months from the filing of the FIR. Considering that similar cases have been pending in other states for a much longer time, the efficient handling of the case which happened to be the first case of the Chennai Cyber Crime Cell going to trial deserves a special mention.

The case related to posting of obscene, defamatory and annoying message about a divorcee woman in the *yahoo message group*. E-Mails were also forwarded to the victim for information by the accused through a false e-mail account opened by him in the name of the victim. The posting of the message resulted in annoying phone calls to the lady in the belief that she was soliciting. Based on a complaint made by the victim in February 2004, the Police traced the accused to Mumbai and arrested him within the next few days. The accused was a known family friend of the victim and was reportedly interested in marrying her. She however married another person. This marriage later ended in divorce and the accused started contacting her once again. On her reluctance to marry him, the accused took up the harassment through the Internet.

On 24-3-2004 Charge Sheet was filed u/s 67 of IT Act 2000, 469 and 509 IPC before The Hon'ble Addl. CMM Egmore by citing 18 witnesses and 34 documents and material objects. The same was taken on file in C.C.NO.4680/2004. On the prosecution side 12 witnesses were examined and entire documents were marked as Exhibits.

The Defence argued that the offending mails would have been given either by ex-husband of the complainant or the complainant her self to implicate the accused as accused alleged to have turned down the request of the complainant to marry her.

Further the Defence counsel argued that some of the documentary evidence was not sustainable under Section 65 B of the Indian Evidence Act. However, the court relied upon the expert witnesses and other evidence produced before it, including the witnesses of the Cyber Cafe owners and came to the conclusion that the crime was conclusively proved. The. Additional Chief Metropolitan Magistrate, Egmore, delivered the judgement on 5-11-04 as follows:

" The accused is found guilty of offences under section 469, 509 IPC and 67 of IT Act 2000 and the accused is convicted and is sentenced for the offence to undergo RI for 2 years under 469 IPC and to pay fine of Rs.500/-and for the offence u/s 509 IPC sentenced to undergo 1 year Simple imprisonment and to pay fine of Rs.500/- and for the offence u/s 67 of IT Act 2000 to undergo RI for 2 years and to pay fine of Rs.4000/- All sentences to run concurrently."

The accused paid fine amount and he was lodged at Central Prison, Chennai. This is considered as the first case convicted under section 67 of Information Technology Act 2000 in India. Source: http://delhicourts.nic.in/CYBER%20LAW.pdf

PResenters of *PReSENSE*

N. Vittal,
Guest Editor

K. Srinivasan
Editor in Chief

V. Rajendran
Strategic Editor

P. A. Narrendiran
Content Editor

Veena Vinod
Podcast Editor & PodJockey

Shvetha Sridhar
Podcast Editor & Pod Jockey

V Poornima
Cartoon Editor

K. Bhavani
International Editor (South Asia)
Singapore

Archana Verma
International Editor (USA)

Deon Binneman
International Editor
(South Africa)
Johannesburg

Awards

Published by
Prime Point Foundation

Feedback and sponsorship
editor@corpezine.com

Past issues may be downloaded from
www.prpoint.com
www.primepointfoundation.org
www.corpezine.com

Listen to India's first pod-magazine
www.poduniversal.com
one stop shop for podcasts on all subjects

To subscribe to this ezine.
http://tinyurl.com/229pyo