eSecure

Secure and be Aware !

An e-zine from CySI

[Volume 1, Number 3]
December 2013

Presidential Address

Dear Readers

We are now launching the third issue of our ezine. So much has happened in cyber security front during the recent past and much is happening. Of course, day in and day out, many cyber-attacks are getting reported. News get publicized. Prevention methodologies keep increasing with better strategies, some techno-based, some law-based and some simply user-based, like creating awareness on the part of users to follow more norms, adopt better Dos and Don'ts and ensure more stringent adherence to regulatory guidelines.

Though it may sound rather alarming if not pessimistic, let me say with guarded caution, it is always better to keep minimum balance in those accounts with internet banking and go in for the absolutely required level of Maximum Credit Limit in the case of credit cards. Normally, credit card issuers canvass for a higher limit in credit purchase and a higher cash withdrawal limit and push it to the users, most often even without being requested for by the card-holders. To minimize the risk exposure, let us not fall for such offers of enhanced limits in credit purchase or cash withdrawals. After all, not that we always need purchase limits in lakhs of rupees or cash requirements in a lakh or so. And in those accounts where there is an Internet Banking facility or an ATM facility, let the balance not be in huge lakhs of rupees. The entire world with thousands of crores of business survived very efficiently without such electronic delivery channels like ATMs, Internet Banking, Cards and Mobile Banking till about two-three decades back. Especially, in a credit card when the card gets cloned and purchase happens from a remote place and the SMS is received and the card owner is shocked….On investigation, the transaction traces to a far off merchant establishment ….just imagine the situation. The card issuing bank may disown the responsibility and it becomes a highly complicated techno-legal issue to prove that the card owner did not use the card and it is a place, often abroad, where the card owner never visited.

All these are points to ponder…..Let us keep discussing these problems and many more such, in the later issues that are to come. As usual, please keep emailing your views frankly to the editorial team.

Rajendran V

*****

Editorial Board

This Issue

*****

At the outset CySI wishes all the readers
A VERY HAPPY AND PROSPEROUS NEW YEAR 2014.
Let the New Year bring lots of peace both in official and personal life of all.

Secure your Credit/ Debit/ ATM Card Transactions (continued from last issue)

When did you last update your e-mail address and phone number with your credit card issuer? Many do not even bother.

Now, imagine being **billed for fraudulent purchases made from your card**. What do you do? First, of course, you **inform the card issuer**, who will probably ask you to fill a declaration form. Doing this quickly is important as, according to rules, if the issuer isn't informed within 30 days of you receiving the statement, it is assumed that you have accepted it as accurate. So, if you were out of station and didn't notice it on time, you would be legally bound to pay.

Of course, if you had updated your contacts with the card issuer and got an alert, which comes within minutes of the transaction, you could have called up the issuer immediately and saved yourself the loss.

Important communication, these days, happens through e-mails, SMSs and phones. Hence, it is crucial that the customer keeps his bank updated so that he can be reached any time for checking a transaction's authenticity.

Common Catches: In India, according to a provision in **credit card contracts**, the card-issuing company isn't liable for any fraudulent transaction unless the customer files a report immediately. Once reported, the card holder is no longer liable. So, be alert and look out for the red flags. Card frauds range from purchases made on lost or stolen cards to phishing, identity theft and traps set up through unsecured Internet transactions.

Skimming or Cloning is something to be cautious about, especially when travelling abroad. In this, data in your card's magnetic stripe is recorded when swiped at a machine. This information is then used to make duplicates. It can happen anywhere, at a petrol pump or a restaurant or any POS. Hence make sure the card is swiped in your presence. To minimize risk, banks also advice customers to replace cards after trips.

Do you use your card online? **Beware of cyber swindles**. These involve unauthorized use of card details, such as the card number, the Card Verification Value, to make purchases online. One should register for online transaction passwords such as Verified by Visa or MasterCard Secure Code and avoid using public computers. Also, make sure that the transaction happens through a secure website, which begins with https.

We will continue with some tips to secure our cards.

Dr. Ramamurthy N

Computer Security Day

30th November is celebrated as **World Computer Security Day** every year**. True to its mission/ vision CySI celebrates the World Computer Security Day in its own way.**

This year we celebrated it in advance on 21st November 2013, at Hotel Savera, Chennai in collaboration with US Consulate, Chennai. This is primarily to match the visit of Mr. Larry Clinton, President & CEO, Internet Security Alliance, US.

A gist of the talk of Mr. Larry Clinton is given below for the benefit of all.

- Every minute globally - 45 new viruses peep in, 200 new malicious web sites add, 180 personal identities stolen, 5000 examples of malware created and on account of all these US$ 2 million lost.
- India's National Crime Records Bureau reports a 50% increase in cyber-crime every year
- India is the 3rd largest producer of SPAM
- The percentage of worms and viruses in India is significantly higher than any of the Asian Pac Rim average
- India ranks 2nd in web based attacks among the Asian Pacific Rim countries
- As in most other countries around the world the cyber security situation in India is one of relative chaos and insecurity arising from periodic reports of espionage, cyber terrorism, cyber warfare and cyber-crime. The complexity of the issue has resulted in a virtual paralysis. Legal and law enforcement mechanisms have not shifted gears fast enough…lack of a coherent policy will seriously interfere with India's national security and economic development.

The magnitude of the problem:

- Technology Changes too quickly.
- Attack methods change too quickly
- Problem is international---beyond any government & international governance is impractical
- Name and shame creates incentive to incentives to attack
- Audits may not improve security and sometimes it could be counterproductive.
- The single biggest threat is from insiders

Majorly of the attacks are of two types:

- Basic attacks
  - Vast majority, Can be very damaging, Can be managed
- Ultra-Sophisticated Attacks (e.g. APT)
  - Well organized, well-funded, multiple methods, probably state supported

How do we approach this problem in a risk management framework? Since the problem is economic an economic solution is needed:

- A cost effective approach will not only provide immediate help but also offers a sustainable solution
- Industry standards and practices has to be relied.
- Government has to provide economic incentives to voluntarily adopt
- An international focus, attention and joint effort is the need of the hour.

Let us be aware of what is happening around us. Wish you all a secure and fruitful computing.

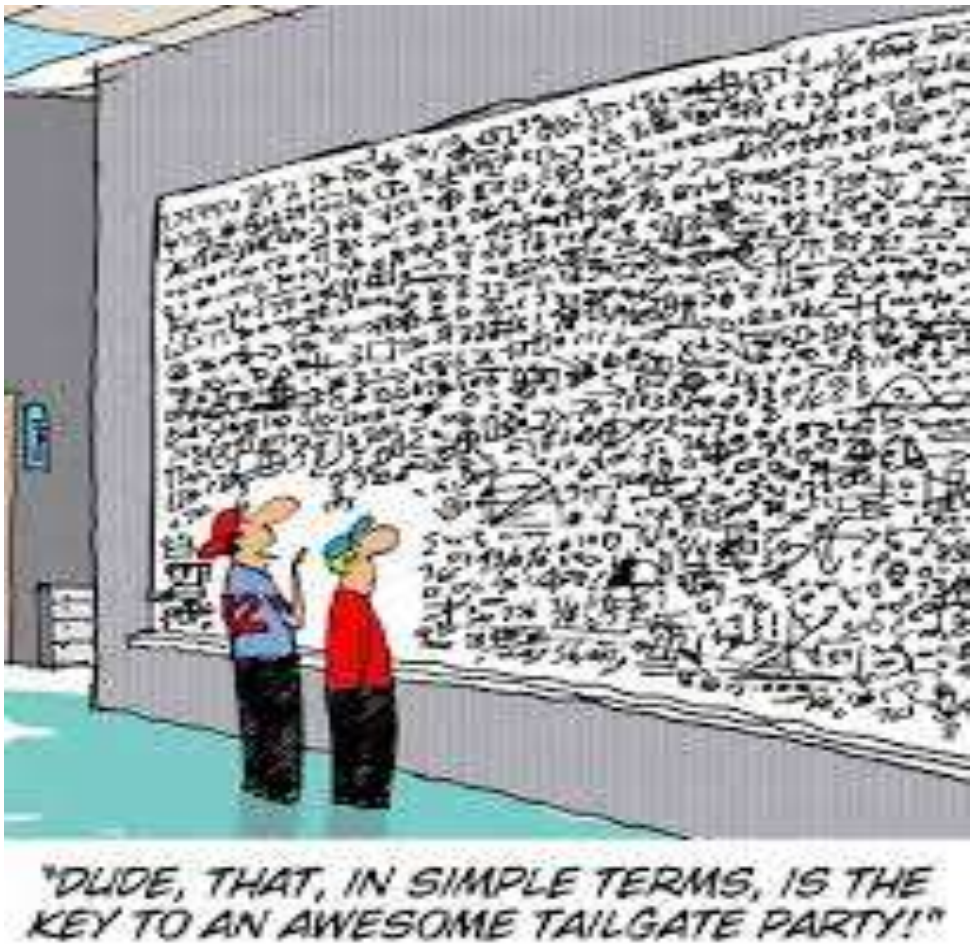
Summarized by *Dr. Ramamurthy N*

*****

Some Interesting Quotes/ Cartoons

Dr. *Ramamurthy N*

These may look funny, but they carry lots of messages. Thanks to the Internet.



P.S. For those who are not aware – tailgating is passing without proper access through an access controlled area behind a person who has access.

Target Foot-printing and the Cyber Laws – Part 2

Having got introduced to the term Target Foot-printing in the previous issue, we shall now look into the methods and implications of FP activities. How is FP done? Most often it is through direct but passive contact, seeking under some guise, information on e-mail ids, phone numbers, location of premises, details of service providers, person's unique identity details, information on the network administrator and so on. The areas targeted by an attacker are wired and wireless networks, DNS, Firewalls and all communication devices.

Going into the sources of FP, it starts from websites, mail ids, online directories, company's annual reports, publications and so on. Open source information are also available in plenty. Whether the target is an individual or a corporate, many information are readily available online.

Many individuals including organizations volunteer to share official and/ or personal info, even highly sensitive ones over the net. Some of the necessary information are obtained merely by sending online queries for which most of the persons even employees respond and share details unwittingly.

Other methods are through web crawling, port scanning and packet sniffing to mention a few. New technologies for intrusion comes up almost daily which makes the job of an attacker easier. The very development of technologies intended for constructive purposes like tracing a digital evidence to investigate a crime or for checking vulnerability of a computer system becomes destructive at the hands of wrong persons.

Some of the tools for FP are, Port scanner, Trace route, NS lookup, Tracert, Search engines, Social networking sites and so on.

The point for discussion now is what our Cyber Laws say on FP activities. There are instantly two wings attached to this question. One is the civil liability and the other, criminal liability arising out of FP activities. This discussion confines to criminal liability. This again divides into FP in violation of law and FP not in violation of any law.

What are the provision of the Indian Cyber laws, the violation of which could possibly be roped in for criminal liability? One strong provision is *If a person dishonestly or fraudulently, without permission* (this includes exceeding permission) *of the owner or any person who is in charge of a computer, computer system or a computer network- accesses or secures access of such computer, downloads, copies or extracts any data, that person shall be held criminally liable and shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both*. It should be noted that liability arises whether or not any consequential loss has occurred. Just as in any other crime, the aspect of *mens rea* or the intention is crucial and the act should have been committed in furtherance of the intention for criminal liability to arise. The terms *'dishonestly'* means to do a thing with intent to cause wrongful gain to one person or wrongful loss to another person. The term *'fraudulently'* means to do a thing with intent to defraud'.

The term *'access'* has a direct implication. It means entry into, instructing or communicating with the logical, arithmetical or memory function resources of a computer, computer system or a computer network. The term '*secure Access'* has a crucial meaning. It means to ensure that access can be achieved at a time desired by the person when he seeks access. A classic example is collection of sensitive data, passwords or any other information without permission of the owner which he could use for committing an offence at a later time. This is a crime by itself. In such a scenario and as per circumstances of each case, it could also be construed as 'attempt to commit an offence'. For this, the enforcing authorities need training on legal and technical aspects of Information Technology.
We shall discuss in detail on the topic in the third part of the article in the next issue.

Padma R.

*****

This ezine and all the previous issues, as well, can be read from our web-site http://cysi.in/.

The contents in this ezine are meant for sharing of knowledge and hence readers are requested to circulate this ezine in full or in part to anyone they like. Probably the readers may like to acknowledge CySI while reproducing the articles.

Readers are requested to send their feedback, articles, jokes, etc., to ezine@cysi.in.

Let us meet in the next issue with more thought-provoking articles.

Disclaimer:

Neither CySI nor the members of the Editorial Committee/ Board owns any responsibility for the views expressed by the authors in the articles. The views expressed are the concerned author's individual views only.

Editorial Board