eSecure

Secure and be Aware !

An e-zine from CySI

[Volume 1, Number 4]
January 2014

President's Column

Dear Readers

Law and Technology - Quite often we find that law is left to interpretation. What is lawful may not be so for others. What is grossly illegal for one may be just a small mistake and perhaps not a punishable crime for others. Law, they say, arguably has many faces and differs, sometimes from person to person and place to place and certainly nation to nation. Inside India itself, what is lawful for a Mohammedan may not be so for others and what is permissible and legal for someone in Tamil Nadu or other states may not be so for one in Jammu and Kashmir or perhaps Assam. But I am not talking about these in this column. I wanted to share some thoughts on *law and technology.* What is pure technology may be treated as unlawful and illegal under specific circumstances.

Cybersquatting is the **act of registering a domain name often with a specific intention that resembles the name of another firm or person already in existence or likely to come into being.** Nowadays it denotes different forms of bad faith registrations. For instance, suppose I know that someone is going to start a million dollar company in the name of say "Good company Enterprises" in the next few months. Knowing this, I immediately register a website in the domain name of "Goodcompany.org" "Goodcompany.in" and with other domain names like "co.in", 'com' etc., by spending a few thousand rupees. When the real company gets incorporated physically with premises and locations, they have to come to me for the usage of these domain names for their websites. At that time, I would demand NOT just a few thousand rupees but perhaps in lakhs.

Another variant of this cyber-squatting is Typo-squatting. It is always possible that Internet users will mistype the name of a Web site (or actually it's URL) when surfing the Web. Typo-squatting is that act of registering domain names with such possible input errors for a "brand name" Web site known for its high traffic and then monitor to see how many clicks a day each of their mistyped domain names receives.

The typo-squatter then uses such information to sell advertising or for other sometimes illegal or obnoxious websites with even pornographic contents. Advertising revenue might come from selling ads to the original site's competitors or by providing redirect pages to related products or services.

Editorial Board

This Issue

*****

Steganography: The technology of hiding a text or a message inside another format, often a jpg picture in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. Viewed positively, it can be called security through obscurity. From a negative and criminal angle, criminals have used this to send text messages when any interceptor (like investigators) may take it to be an innocuous picture only.

Similarly scavenging. When we buy a new electronic gadget like a mobile or a photocopier, we surrender our old used photocopier (which nowadays come with storage and hard-disks) or the mobile handsets under buyback scheme. The buyer takes the data from the old devices and uses them. Or misuses? This is scavenging.

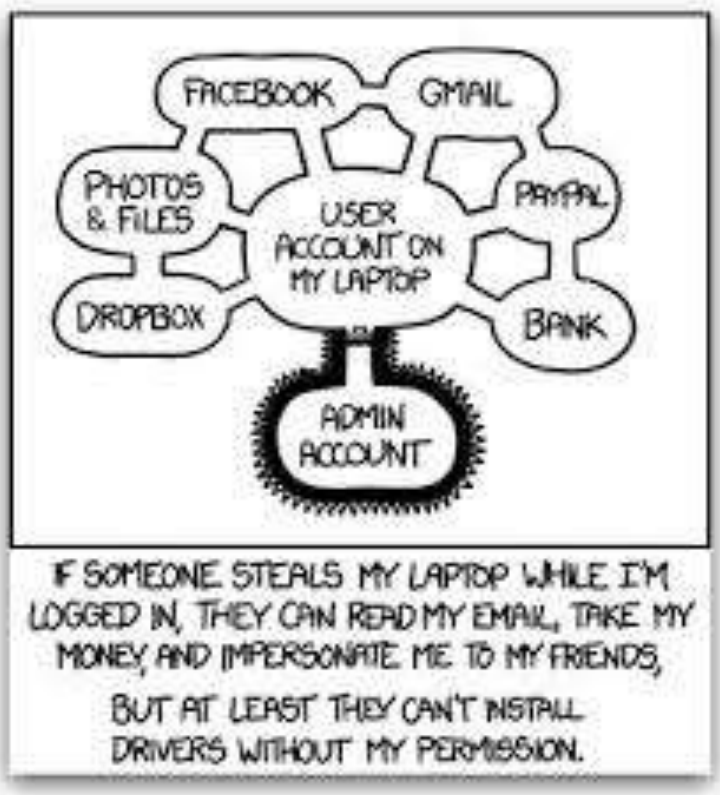
DoS: Denial of Service attacks is just a software program that generates thousands of or millions of queries every second and sends them to a particular server, with a specific intention that the server should not be available to genuine users who may access it at that time. DoS has been specifically mentioned in the Information Technology Act, though the other activities mentioned above are not.

In all these cases above, cybersquatting, scavenging or steganography are all just technologies and per se, are not punishable under any law. But when committed, then the act of personating or cyber stalking or blackmailing or abetment to crime and such related illegal activities, these technologies become a crime.

As usual, please keep emailing your views frankly to the editorial team.

Rajendran V

*****



*****

Editorial

Secure your Credit/ Debit/ ATM Card Transactions – Part 3 (continued from the previous issue)

Fraudsters also try **account takeovers and identity theft**. This happens in two ways:

- One, a cardholder's information is stolen and used for transactions where the card's physical presence isn't required, such as online purchases.
- Two, by placing a request for a new card using the stolen information. Monitoring your credit card report is your best defense.

Always "Check for unusual transactions, especially small ones, as fraudsters make these to check the card's validity,"

Last but not the least, do not fall prey to **phishing mails** (that appear to be sent by an institution you deal with but are not), SMSs or calls.

FRAUD CONTROL:

Usually, banks have dedicated transaction monitoring units and fraud detection systems to analyse suspicious patterns. So, if two transactions are made from different countries with the same card within a short period, the system will highlight this. However, it helps if the customer is also cautious. For instance, opting for cards with signature lamination and a photograph, registering for transaction alerts and transacting only through secured websites are common precautions.

If you are a frequent user, it may make sense to go for an insurance cover to take care of liabilities from loss and misuse. Banks usually have tie-ups with insurers. General insurers also offer standalone credit card policies, which cover all cards held by a customer under one policy. One alert to the insurance company can block all your cards, limiting your loss.

FOR YOUR GRIEVANCES:

The RBI has appointed an ombudsman for redressal of complaints which your bank has failed to respond to satisfactorily. A bank must respond within 30 days from the date you lodged the complaint. In case of wrongful billing, the card company should provide documentary evidence within 60 days. If unsatisfied, the cardholder can go to the ombudsman.

Safe checklist:

HANDLE WITH CARE

- Check your credit card statement details carefully and opt for SMS/e-mail alerts.
- Never defer calling your credit card company if you do not recognise a transaction.
- Always keep your contact details updated with your card-issuing company.
- Transact only through secure websites which have https in their URL address.
- Keep a low-limit card for online transactions and choose a chip-enabled card

Dr. Ramamurthy N

*****

Governance & Cyber Assurance

The Need of Enterprises of Tomorrow:

Prof. Dr. Subramanian K.

Dr. KS, Ph.D., SM (IEEE), SMACM, FIETE, SMCSI, MAIMA, MAIS, MCFE., Former President of CySI, was the first Director and Professor at Advanced Center for Informatics and Innovative Learning (ACIIL) at IGNOU. One of the founder creators of National Informatics Center, under the Ministry of Communications and Information Technology, Government of India and served there for 32 years. Was the I.T. Adviser to CAG of India, associated with IT/ Systems/ ITES design and Implementation and monitoring of major IT Projects of Railways, Police, Banking and many other government departments and private corporate in India.

Internet, Globalization, the Information technology and web technologies have made the world flat today as a global village, transcending political and national boundaries. They interconnect people all over the world in the virtual world of cyberspace-- the virtual space behind the computer screen. Innovations in communications technology keep us all wired 24/7. Cyberspace is currently used for social interactions and networking through emails, instant messaging or video telephony. It is also fraught with threats from organized criminals of the cyber underworld running an underground cyber economy. There is thus a need for governing this virtual world to support global social, political, economic collaboration and exchange while managing associated risks. The objective is to provide trustworthy and efficient computing in cyber space, calling for an effective governance of cyberspace. This is a paradigm shift from eSecurity to eAssurance in cyberspace. This paper outlines the ramifications of governing such a cyberspace that impacts individual human life, social life, global business and governments on such a massive scale in a borderless world and describes the different facets of cyber governance. Ultimately cyber governance must lead to cyber-assurance.

1.0 Cyber/Business Assurance-A Multi-layer Architecture & Paradigm

The business world has changed a lot, from "*doing things rightly*" it has become "*doing right things*". Administration and assurance go hand in hand. Today the requirement is not only for the professionals who can work efficiently themselves but can make the whole system to work smoothly by providing it the secure and healthy environment to the persons around him. For this one main requirement is to have a system wherein we can detect even the smallest frauds and defects that are affecting the organization and its culture because one person is enough to sink the organization."*Technology makes it possible for people to gain control over everything, except over technology*"-- John Tudor. There is an immense need for catering to integrated integration of multi-located, multi-state enterprises.

They are - Operational Integration, Professional Integration (HR) and Emotional/ Cultural Integration

The Critical Issues in Managing inter-dependencies are:

- Critical Is Infrastructure characteristics (Organizational, operational, temporal, spatial)
- Environment (economic, legal /regulatory, technical, social/political)
- Coupling and response behavior (adaptive, inflexible, loose/tight, linear/complex)
- Type of failure (common cause, cascading, escalating)
- Types of interdependencies (Physical, cyber, logical, geographic)
- State of operations (normal, stressed /disrupted, repair/restoration)

In order to tackle these issues in an integrated fashion, a multi-layer integrated framework for Business~ Cyber Assurance is architected.

2.0 Key areas of Assurance:

- Organizational - Systems in place to identify & mitigate differing risk perceptions of Stakeholders to meet business needs
- Supplier - Confidence that controls of third party suppliers adequate & meets Organization's benchmarks
- Business Partners - Confirmation that security arrangements with partners assess & mitigate business risk
- Services & IT Systems - Capability of developers, suppliers of IT services & systems to implement effective systems to manage risks to the organization's business.

3.0 Benefits of Business Assurance:

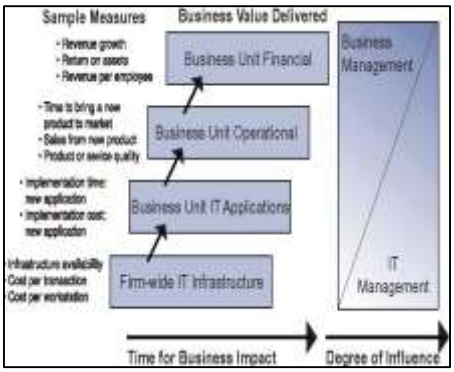
- Supports informed decision making at management and Board level
- Identifies and exploits areas of risk based advantage
- Ability to aggregate business unit risk in multiple jurisdictions & locations
- Demonstrates proactive risk stewardship
- Establishes a process to stabilize results by protecting them from disturbance
- Enables independent directors to decide with comfort and confidence
- Contributes to effectiveness & efficiency of business operations
- Ensures reliability & continuity of information systems
- Assists in compliance with laws & regulations
- Assures that organizational risk exposure mitigated
- Confirms that internal information accurate & reliable
- Increases investor and lenders confidence

Information Assurance has become a very important issue in assuring integrity of Information flowing through multi systems and multi-channels and multi-environments.

Increasingly, the goal is not about information security but about information assurance, which deals with issues such as data availability and integrity. That means organizations should focus not only on risk avoidance but also on risk management, Jane said. "You have to be able to evaluate risks and articulate them in business terms --Jane Scott-Norris, CISO at the U.S. State Department

4.0 IT and the Business alignment - as a function of understanding and properly managing the "seven Ps" – people, process, platforms, products (and services), projects, planning and portfolios.

Moving Up the Value Chain



CySI's Updates

Sri **Ramesh Bhashyam, secretary of CySI** has been selected as one of the Next Gen Top 100 CIOs of the nation. In a contest participated by thousands, only around 2500 were selected for consideration. He came within the top 10 and in a glittering ceremony in Bengaluru, he was honoured. Please join all of us, in congratulating him and wishing him many more such laurels in future.

CySI observed the World Computer Security Day on 21st November 2013, at Hotel Savera, Chennai in collaboration with US Consulate, Chennai. Mr. Larry Clinton, President & CEO, Internet Security Alliance, US, gave an awareness talk. The details of his talk has already been published in our last issue.

CySI organized a meeting of its office bearers and members in the editorial board of the CySI eZine, at the Cosmopolitan Club, Chennai, on 02nd January 2014, on the occasion of the visit of Dr. K. Subramanian (KS) a distinguished member of CySI from New Delhi. The well attended meeting was kept under rapt attention by KS, who walked the attendees through his journey of early years from his association with the Rangarajan Committee for Banking Automation in the year 1982 to the need of the hour.

*****

Dummy's Corner

From this issue onwards, it is proposed to answer some questions – these may seem silly, but these carry lot of messages. Also they are meant for laymen and not for experts.

Q 1. *I am saving all my important information like Internet Banking password in my personal Email- Is this advisable?*

Answer: Saving the Internet Banking password (or any confidential information with financial implication) is absolutely NOT ADVISABLE. The email password is generally not strong enough and does not travel through en encrypted communication (Internet Banking site is on an EVSSL i.e. Extended Validation Secure Socket Layer, represented by a green band in the URL of the bank and the password or the OTP also is always encrypted while in transit). Email password is easily hackable. It is extremely RISKY to store any confidential information in email. In some of the social networking sites and communication sites, we also sign an agreement (like in viber, Skype etc., which nobody reads) enabling the provider to legally access the contents and many other such privileges. Hence DO NOT save any private information involving financial or other criticality in any email.

Q 2. *My brother is in the habit of using the option 'Remember the password' and urges me also to do the same. Can I follow his advice on this?*

Answer: "Remember the password" should never be ticked in a third party's PC or a system in an office or in a public place. By choosing this option, the browser in the particular computer (PC) saves it and gives you the access to the email, even before you type the password. Only when you are sure, it is your own personal PC and you ALONE are going to use it, you can choose the option. Even then, one never knows, when there would be an occasion of telling some visitor to use the system, in which case, the moment the visitor uses the system and goes to the mail, the system will prompt him for your email id and your password, even before his/her typing his/her email id. The visitor is thus tempted to use your email. Hence I would personally say it is NOT ADVISABLE at all to select the option. Always better to type the user id AND the PASSWORD.

Answers by ***Rajendran V***

Some Interesting Quotes/ Cartoons

This may look funny, but it carries lots of messages. Thanks to the Internet. Technology has advanced. No need manual thieves.

Cyber Threats in Internet Banking

Conventionally, we all wake up and have a refreshing cup of coffee in the morning. Of late, most of us wake up with a coffee and at least one Good *morning* SMS probably with a link to a website also. Did anyone of us delve into the roots of our *Good morning* SMS with the following points?

- ✓ Has the sender really sent the SMS?
- ✓ Had it been delivered with the same text as the sender had sent to you?
- ✓ Are we sure that no one has read the message before it was delivered to us?
- ✓ Had the message been delivered intact to your inbox?

If the answer to any of the above questions is NO, then it is believed that we are under the attack of **SMiShing.**

SMiShing is defined as follows: *"Smishing is a form of criminal activity using social engineering techniques similar to phishing. The name is derived from 'SMS phishing'. Smishing uses cell phone text messages to deliver the "bait" to get you to divulge your personal information."*

The same concept to deceive a customer or an internet banking user, is called as phishing. In phishing, the customer of the bank (and in most cases sadly the banker himself) loses the money by disclosing their internet banking login ids and passwords to an unknown fraudster thinking that it is a valid internet banking website. Now let's see the mechanism of a phishing attack.

- ✓ Customer receives an e-mail which reads as below:

Dear Customer - Thanks for banking with xyz Bank. Please click on the below link to update your internet banking details. This is COMPULSORY as a part of our latest security measure in compliance with the recent RBI guidelines.
http://www.xyyz.in/internet-banking.html

Wish you a wonderful day ahead! Regards
Internet banking Administrator

- ✓ As a prudent loyal customer of the bank, the customer clicks the link, enters login id, password and pin number. Alas! He has given the key of his house and locker to the thief now. Yes! The password and the pin number which is to be preserved more precious than your house and the locker keys are shared to the hacker who is actually thief in literal meaning.

But how will the poor (rather RICH) customer know that this mail is a fraudulent one and not sent by the bank? Here are some clues for the same.

- ✓ Check for the GREEN BAR in the top of the browser(Browser is nothing but your Internet Explorer or Firefox) while using internet banking
- ✓ Look out for the YELLOW padlock icon at the bottom right corner of the browser.
- ✓ Be cautious to use https links rather than http links.
- ✓ In the above sample email, if you look closer you will find that the name of the website is xyyz.in instead of xyz.in.

If you feel that the above points are wacky to you, the best way is to type the address in the address bar and use your net banking. The rich online experience unquestionably enlightens the online customers when the security measures are well understood and observed.

Panchi S.

Target Foot-printing & Cyber Laws – Part 3

What if FP is done not-in-violation of any law? Assume that a person collects information of his target through open source, public domain, where there is no need for permission from the owner. This may be done through direct methods, without committing any breach of security measures (like hacking). Also, if he has not, for this purpose, violated any laws in force and has not violated any employer policies, agreements, license, etc., what would be the liability? The answer is - there are no provisions in law to hold him criminally liable. The only possible recourse would be to investigate if there has been an attempt to commit a crime. It is well settled law that merely wishing to commit a crime is not an offence. This is natural justice too.

It has very recently been reported in newspapers about an online bank fraud to the tune of lakhs of rupees. On arrest of the person and seizure of his laptop, it was found that apart from other crucial evidences connected to the crime, five lakh e-mail ids were stored on his laptop. Even if they were not misused so far, there was every possibility of misuse at a later time. X cannot merely file a complaint that Y has web crawled, collected information and is in possession of his e-mail ids, bank account numbers, any unique identification or sensitive data. There are no provisions in law for taking any action.

The law enforcement agency at best, could only investigate if any attempt or abetment of any cybercrime has taken place. But it should be borne in mind that our cyber laws are strong enough to deal with FP activities which have taken place in violation of security and privacy measures of any computer system or network.

FP is not an offence in most of the countries. It is sometimes seen as a preparatory act to commit another cybercrime. But some countries do provide penal sanctions for FP activities.

The real problem in the cyber world is the speed, anonymity, gravity and far reach with which a crime can be committed in a jiffy. So it is imperative that corporates, companies, institutions, association of persons and also individuals take routine measures to check for any remote access capabilities and unusual FP activities in every sphere of cyber space. They also need to implement network based detection systems, look for malicious activities and take corrective action. This is important because in addition to the attack and risk of financial loss and/or loss of data, the target may also end up with other civil and criminal liabilities unwittingly. Employers should hire persons after a background check. It is advisable to impart training on the legal aspects to groups of employees, create awareness and also allot funds for implementing necessary safety standards lest the companies become liable for paying huge damages and face prosecution.

Certain measures could be taken to prevent FP activities. Restrict information on a company's website and its network information to a minimum. Disable unnecessary services on the internet - more the openings, more the chances of attack. Avoid providing too much specific information about the domain name or collective network. Avoid wild net surfing. Change the technology framework and other security measures periodically so that even if any FP has taken place, an attack attempt at a later time can be rendered futile. Enforce implementation of best security practices at all departments of corporate houses. Encrypt messages, particularly sensitive ones. Use digital signatures wherever possible. Needless to say, be discreet in sharing information through internet, more so on social networking websites.

Being secure in the cyber world is in our hands. After all, when we hear of series of thefts in a locality, we do not throw open the doors and run away. Instead, we go in search of stronger locks to keep the houses safer. The same doctrine applies in cyber world too. The need of the hour in our country is to develop indigenous hardware and software technologies encompassing all requirements of networking and operating systems, which could be held completely under our control.

Padma R.

*****

CySI wishes all the readers
A VERY HAPPY SANKARANTHI

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