# PRSENSE

Communicate the communication

**India's First Corporate ezine**

**Issue No 38 – Apr 2009**

**Published by Prime Point Foundation**

**Theme of this Issue**

**Computer Vulnerability**

**Guest Editor**

**M L Srinivasan**

**M L Srinivasan**
**IT Security Expert**

**In this Issue:**



**Contact**

www.corpezine.com

editor@corpezine.com

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

# Use Technology; but guard yourself

Presently, Technology has grown enormously. All of us use desktop computers, laptop in different operating systems like Windows, linux, etc. All of us spend more time on internet. Every day, new virus gets circulated and all the computers in our office and at home are not safe. Without your knowledge, the data can be stolen from your system. Even the firewalls cannot prevent this. There may be some hole in your system, through which, the data can go out.

The online financial transactions also nowadays pose greater risk. Vulnerabilities in the Banking sites have enabled the hackers to spread their worm to the online users. Many users get cheated through fake emails asking for id and passwords.

More we use the Technology, more we will be exposing ourselves to a greater risk. A new terminology like 'Cyber terrorism' has also come into usage. In spite of all the various threats, sadly, there is less awareness amongst the Corporates and the users about the security of their own transactions. While, we cannot stop the growth of the technology and our usage, we need to guard ourselves from the bad effects of technology.

In the interest of the general public, this issue will deal with the fundamentals of computer vulnerabilities and how to protect ourselves from this 'greatest' risk. We want to create an awareness. We are fortunate to have Mr M L Srinivasan, a well known Security Expert to Guest Edit this issue.

K. Srinivasan

### Guest Editor

Mr M L Srinivasan, Founder and CEO of ChennaiNet is globally well known InfoSec professional and trainer on Information Security in India. He has written many articles on Information Security and has also authored a book. He is also ISO Auditor on Information Security. He can be reached at mls@chennainet.in

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

# Corporates lack awareness on vulnerabilities

Today we buy software across the shelf and/or the computer that we buy comes with the software pre-installed in it. The most important of all the software that are used in a computer is its 'Operating System' in short the OS. Without an operating system a computer is non-functional. Most popular operating systems are Microsoft Windows, Redhat Linux, BSD UNIX, Sun Solaris etc., The operating systems are divided as Server and Desktop. What we normally use on our desktops and laptops are desktop OS. The most popular OS in this category is Microsoft Windows which is installed in nearly 80% of the desktops Worldwide.

There are critical vulnerabilities in the desktop operating systems as well as server operating systems. Vulnerabilities are prevalent in many of the applications such as Microsoft Office, database systems such as Oracle, Internet browser such as Internet explorer, Mozilla Firefox and so on. Hackers, viruses, worms and trojan horses target these vulnerabilities to compromise the systems. Organizations install anti-virus packages to combat viruses and worms. But they seldom patch their systems against the vulnerabilities. If the vulnerabilities are identified regularly and the systems are patched, then the incidents of virus attacks and hacking of the systems will drastically come down.

There is a lack of understanding of security issues in most of the corporate. Vulnerabilities are the root cause of many IT security issues. Periodical scanning and patching of the IT systems will ensure that the systems are less prone to compromise due to a virus or hacking attack.

M L Srinivasan

**Non compliance of Security issues at Corporates may lead to (1) Monetary loss, (2) Loss of customer confidence and (3) Legal problems. Please listen to the exhaustive podcast interview at**

**www.prpoint.com/security**

# Top Ten IT Security Issues

## An overview of IT security issues we face today, the future trends and possible actions.

### 1. Cyber Attacks

The Internet or World Wide Web (WWW) is also called Cyber Space. This space connects various computer networks across the World (and in future in other planets that we occupy!!). Like each individual, each network is distinct in terms of the IT systems used, the way it is setup, configured and managed. This heterogeneous nature has many weaknesses that are prone to attacks. Cyber Terrorism, Cyber Warfare and Cyber vandalism are some of such attacks. Many such attacks are happening today albeit less in magnitude and in the future we may face high intensive attacks that could cripple the cyber space.

Co-ordinated efforts from Computer Emergency Response Teams (CERT) across the World with timely alerts to user communities could mitigate risks from this threat.

### 2. IT Vulnerabilities

Vulnerabilities in IT systems are holes or errors that are exploitable. They are there due to poor design or poor coding or both. When vulnerability is exploited, it results in security violation such as compromise of the IT system, service disruption or obtaining higher privileges. Vulnerabilities are the root cause of many of the security issues mentioned in this column.

Efforts such as Common Vulnerabilities and Exposures (CVE), National Vulnerability Database (NVD) etc., provide glimmer of hope for combating and reducing them in the future. Based on the knowledge learned from various hacking/virus/worm related incidents it is quite possible to develop secure systems by following secure coding practices.

## 3. Lack of Monitoring, Security testing and User awareness programs

Though this is an organizational issue, monitoring of suspicious activities in the network is performed using IT systems. Information Security is predominantly based on preventive and detective controls. Monitoring assists in devising proactive and reactive actions based on events. Security testing involves vulnerability assessment, penetration testing and security policy audits. The trends indicate that many organizations lack or do not follow such procedures.

User awareness in terms of Do's and Don'ts based on organizational security policy must be created. These three activities if followed regularly would minimise the risks from all the other issues mentioned in this column.

## 4. Identity Theft

Identity theft refers to stealing one's identity for wilful gain such as money, fame, and power and for criminal activities. A simple identity theft is stealing a password. Banks and financial institutions are defrauded by impersonation; confidential data are stolen from Government, Military and Corporate for terrorism, warfare and espionage due to identity theft. In the future this issue will assume gigantic proportions as more and more devices join the network bandwagon and establish their identity besides humans.

Digital certificates, Biometrics such as finger print, voice, face and retina recognition systems, and Radio Frequency Identification Devices (RFID) are some of the effective solutions to this issue and we can expect much advancement in this area.

## 5. Malware

Refers to (Mal)icious Soft(ware) and as the name implies, the purpose is to cause harm to the systems or steal information. Viruses, worms, spyware such as key loggers, Trojan horses, root kits etc., are examples of malware. The present trend is alarming and statistics show that hundreds of billion dollars are lost due to malware. Another statistics show that more than 50% of online users have reported spyware infection to their systems. Malware exploits system vulnerabilities and human weaknesses. Organized crimes such as planting malware in legitimate websites like online banking that gets automatically downloaded to the computers of the innocent users are on the rise. Technologies like Web2.0 also prone to malware infestations.

Future trends indicate more sophisticated malware and require heightened awareness as well as using legal copy of operating system, anti-virus and personal firewall by the users.

## 6. Botnet

**Botnet refers to malicious networks managed by Computer Robots. They compromise vulnerable computers (called as zombies) in the network and use them for attacking other computers, stealing information, storing and transmitting illegal data such as porn movies or pirated and malicious software. We see proliferation of distributed botnets that automatically switches the controlling computer robot to another computer or network in case of network block by the service provider/law enforcement agencies. This trend is going to increase more and more and controlling botnets will be a big challenge. There is an unofficial estimation that one quarter of the computers connected to the Internet will be compromised and become part of botnet. User awareness and periodical vulnerability and activity scanning of computers is a must for combating this threat.**

## 7. Unsolicited Commercial Email

**Spam as is popularly known is an issue that drains the network resources such as bandwidth and storage space. Besides, many human hours are wasted in download time and trashing such emails. Important security issues are that spam is used for phishing, pharming and distribution of malware. The root cause of the problem is the way email is being transported and exchanged across millions of mail servers across the world and the weak spam controls. The present trend is more on using zombie computer to send spam as more and more service providers are shutting down spam servers. However, many of the spam originate from servers hosted in countries like Russia, China and Philippines.**

**Using spam filters, and co-ordination from the countries that do not have stringent laws against spam, is the way to go for solace from this menace.**

## 8. Mobile and wireless attacks

**The business and user community increasingly adopts mobile devices and wireless networks. Mobile commerce such as banking, shopping, etc are seeing rapid advancements. Common attacks that are perpetrated against such devices and networks include Bluetooth attacks, SMS Spoofing, Smishing (**SMs phISHING**), compromising the WEP keys as well as setting up ad hoc networks. In future, attack sophistication and vectors are bound to increase and this is one area that is going to give constant nightmare to IT and Security professionals.**

**User awareness is the key to prevent many such attacks besides stronger authentication mechanisms.**

### 9. Web based Social Engineering

**Social engineering refers to the art of inducing a user to inadvertently perform an action for the purpose of obtaining sensitive information such as passwords, credit card or bank account information etc. Web based tactics involve spoofed emails that appear to have come from legitimate entity such as your bank asking for personal details, Nigerian scam, illegitimate websites constructed in such a way with a look alike of a legitimate site or in the form of giving away free software, music, video etc.. Advent of social networking sites, instant messaging and mobile phone based internet communications are some of the hot spots that will spur this activity to dangerous levels.**

**Humans are the weakest link in a security chain. Common sense approach to any access or communication with known/unknown entity on the web must be practiced.**

### 10. Peer-to-Peer File sharing

**This refers to communication between two or multiple computers directly for sharing files such as software, music, video etc. Since this activity involves direct access to the file system of the shared computer, the chances of implanting malware is very high. The concept of trusted source in such system is weak. Criminal networks operate in this domain that perpetuate organized crime. The trends are more geared towards underground suspicious activities.**

**Participating in an insecure peer-to-peer file sharing networks is to be avoided.**

## BE WARE AND BE AWARE OF LAW GOVERNING YOUR COMPUTERS

### Information Technology Act 2008 - India

**Section 43A**

**Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.**

**(Similar clauses are also there in other countries like US, UK)**

# PRince

BY - TRIAMBAK SHARMA

www.cartoonwatchindia.com
cartoonwatch@gmail.com

I TOOK SERVICES OF 'HACKER' & REVEALED THAT YOU HAVE KEPT YOUR PASSWORD IN NAME OF YOUR GIRL FRIEND... & NOT MINE

IF YOU WANT TO KNOW MY CORRECT AGE... TRY TO FIND MY 'PASSWORD'

## TEN COMMANDMENTS FOR COMPUER USERS

01. **Use only legal version of Operating Systems, Softwares and antivirus. Pirated OS and software may harm your computers and your data is prone to be stolen. Update the patches periodically.**

02. **Never transact e-banking from a public places like Cyber Café. Your id and password could be stolen through key logger software hidden in the computers.**

03. **No Bank will ask for your id and password through mail. When you receive such mails, do not follow the hyperlinks given in such mails. Do not give your details to unauthorized sites. Login directly through the official site of the Bank and transact.**

04. **Generally, keep a complicated and strong password for all your transactions (mails, financial, etc.). Never use your name or the names of family members or sequential numbers like 12345, etc.**

05. **Do not keep the record of your password anywhere. Keep in your mind. Storing your password in your desktop or laptop is also risky. Always type fresh every time when you login.**

06. **Do not open any attachments without scanning for virus, even when it comes from known sources. Do not forward the attachments to others, without scanning for virus. They are likely to contain malware to harm your system.**

07. **Even if you configure spam filter to separate spam mails, do not delete spam mails, without verifying once. Even genuine mails may be found in spam box.**

08. **Use a software based firewall. Many such firewalls are free for Home users.**

09. **Use legal version of anti virus software and set 'automatic update'. Perform full system virus scan once in a week. Use anti spy ware software to periodically to check infections.**

10. **Use plugins like Google toolbar for Internet explorer or firefox that has built in capability to warn potential malware or phishing websites.**

## Important Podcasts of this month at www.poduniversal.com

| | |
|---|---|
| Leadership defined in Bhagwad Gita | www.prpoint.com/pod1 |
| What prompted Jarnail Singh to throw shoe on Indian Home Minister? | www.prpoint.com/pod2 |
| Music breeds success – All about Music | www.prpoint.com/pod3 |
| UnSung Heroes – Bhumi Chennai | www.prpoint.com/pod4 |
| Media students interact with Mr T S Krishnamurthy, Former Chief Election Commissioner of India | www.prpoint.com/pod5 |
| N Gopalaswami, Former Chief Election Commissioner, a 'Role-Model' in Indian Civil Service | www.prpoint.com/pod6 |
| PR Icon – Vikam Kharvi, Mumbai | www.prpoint.com/pod7 |

## Free Online Virus, Trojan Horse and Malware scanners

| | |
|---|---|
| Symantec Security Check | www.prpoint.com/symentec |
| McAfee FreeScan | www.prpoint.com/mcafee |
| Kaspersky Online Virus Scanner | www.prpoint.com/kaspersky |
| Panda ActiveScan 2.0 | www.prpoint.com/panda |
| Avast! Online Scanner | http://onlinescan.avast.com/ |

# PRCI Global Meet

**Public Relations Council of India (PRCI) organised 3rd Global PR Meet, *"PRoActive"* at Bangalore on 3-4 April 2009. During the event awards were given under various categories for excellence in PR and Communication.**

**The following 11 Public Relations professionals were inducted into PRCI HALL OF FAME AWARDS 2009**

**(1) K. N. Ashok Kumar, Bangalore (2) Charanjith Singh, Chandigarh (3) Geetha Shankar, Chennai (4) B. N. Garudachar, Mumbai (5) Krishna Baji, Hyderabad (6) B N Kumar, Mumbai (7) KRM Reddy, Bellary, Hospet (8) B K Sahu, Kolkaa (9) Shivananda,New Delhi (10) Vishwanath Pandey, Varanasi (11) G P Jayakumar. Chennai**


**Mr. Charanjit Singh, Managing Director, Core PR, Chandigarh is seen receiving Honour inducting him into Hall of Fame 2009**

**Ms Geetha Shankar, Chennai is seen receiving the Honour**

**Mr Krishna Baji, Hyderabad is seen receiving the Honour**

## GFPR Foundation Day

**Global Forum for Public Relations (GFPR) celebrated their Foundation Day on 21st April 2009 at Hyderabad. They organised a Seminar on *"Election 09 – Role of Media"* with many eminent media persons sharing the views. Every year, GFPR presents the Golden Triangle Award to one outstanding Communication professional. The third of such Award was given to Mr M B Jayaram, Chairman Emeritus, Public Relations Council of India (PRCI).**

**In the photo Mr Jayaram is seen receiving the Award from Sri Devulapalli Amar, Hon. Chairman Press Academy, AP. Mr B K Karuna, President of GFPR looks on (second from left)**

## PR-eTTY

### 'Excellence' is a drive from inside, and not from outside

**A German once visited a temple under construction where he saw a sculptor making an idol of God. Suddenly he noticed a similar idol lying nearby. Surprised, he asked the sculptor, "Do you need two statues of the same idol?" "No," said the sculptor without looking up, "We need only one, but the first one got damaged at the last stage." The gentleman examined the idol and found no apparent damage. "Where is the damage?" he asked. "There is a scratch on the nose of the idol." said the sculptor, still busy with his work. "Where are you going to install the idol?"**

**The sculptor replied that it would be installed on a pillar twenty feet high. "If the idol is that far, who is going to know that there is a scratch on the nose?" the gentleman asked. The sculptor stopped his work, looked up at the gentleman, smiled and said, "I cannot install the statue when I know it has a defect."**

**The desire to excel is exclusive of the fact whether someone else appreciates it or not. "Excellence" is a drive from inside, not outside. Excellence is not for someone else to notice but for your own satisfaction and efficiency…**

**Source: Unknown**

## PResenters of *PReSENSE*

**M L Srinivasan**
**Guest Editor**

**K. Srinivasan**
**Editor in Chief**

**V. Rajendran**
**Strategic Editor**

**Narrendiran**
**Content Editor**

**Triambak Sharma**
**Cartoon Editor**

**Veena Vinod**
**Podcast Editor & PodJockey**

**V Poornima**
**Coordinating Editor**

**K. Bhavani**
**International Editor (South Asia) Singapore**

**Archana Verma**
**International Editor (USA)**

**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.**
**www.prpoint.com/PR-e-Sense**