

## **Computer Forensics or Junk Science?**

### **Introduction**

Cyber crimes are here to stay. It is not unusual to come across articles / debates on data security, privacy, vulnerability, identity theft, online credit card frauds etc. This is the negative side of the internet which is an intrinsic part of our lives.

Computer forensics, often called junk science is the emerging and rapidly changing science of analyzing computer crimes, understanding and interpreting the evidence with the emerging legal systems that apply to different countries. Computer forensics most certainly goes beyond being a geek preserve as it involves people from diverse backgrounds such as law makers, law enforcers, financial specialists, domain/industry specialists and IT professionals.

### **Cyber crime boundaries**

Cyber crimes occur mostly within the enterprise network or on the internet itself. Both these environments present opportunities for cyber crime to happen since computers were not built with the internet in mind nor are people trained adequately to protect themselves when accessing the net.

Cyber crimes range from simple hacking, identify thefts, destruction of data, intrusion of privacy, piracy, application hijacking or stealing of valuable enterprise information. Detection is a big challenge since individual users could log in from anywhere and portable notebooks/USB storage devices only make it harder to detect.

### **Monitoring vs. Compliance: Role of the ISP**

It is almost impossible to police the net although a lot of control can be vested with the regional feeder networks and ISPs. There is public debate on how appropriate logs and trails can be maintained and leveraged as evidence.

The challenge always remains in achieving balance between monitoring and user compliance and process, solutions and laws seem to be still a long way off from a workable solution. As an individual user of the internet, we have to contend with legal aspects of content, protecting data on our hard disks from malicious programs (viruses et al), understanding what terms we sign up for (end user agreements), doing online commercial transactions on the internet and ensuring safety of data that we transmit on the internet.

The ISP has a large role to play to ensure a safe harbor for the transactions, data exchanges and making users aware of the issues and challenges whether the user is at home or in a cyber café.

### **Data security & privacy**

The modern enterprise is the single biggest commercial user of the internet and today businesses run 24/7/365 owing the ease of connectivity and ease of information availability. Enterprises today protect themselves by deploying

private networks and thereby limiting outside interaction to fewer machines. However the biggest threat to the enterprises is the traveling executive who is accessing information through various devices – in fact working on a wireless network in an airport/hotel is the easiest way to get hacked!!

Electronic surveillance is now an accepted method of protecting information and companies try to balance between ensuring data privacy (emails, voice mails) and ensuring enough levels of backups/offsite storage to recover quickly from any impending disaster. Failure to comply with information security and intellectual property protection norms results in termination and helps in being a deterrent. The bigger challenge in the enterprises is with the end user community in government sector, defence, public utilities and financial sectors which are the typical target for cyber crimes.

The individual user on the internet is even more vulnerable owing to the awareness levels, availability of software to protect home users and also monitor usage. The only way this could be achieved is through education, awareness, training and a strong legal framework to take on people who do not comply.

### **Emerging Legal Frameworks**

Across the world, there is increasing awareness of cyber crime. Some of the emerging acts and statutes include the Sarbanes-Oxley, Gramm Leach Biley, US Patriot Act, USA Patriot Act, HIPAA, Basel II and the Information Technology Act in India. It would be useful to read case studies that explain how we could protect ourselves and our data/intellectual property.

### **Protecting ourselves**

Individual users need to look for tools, software and process to address protection (authorization, authentication, encryption, physical access restriction etc); detection (data history and reporting compliance); business continuity & response plans (to recover from any such situations).

Most important of all is to be sure of the information that you are sharing in cyberspace especially people whom we do not know or have not interacted with. The biggest threat that all of us will have are with financial transactions and that is where we need to be real careful about identity theft.

### **The final word....**

Cyber crimes are going to be a part of cyberspace. Just imagine what we would have to contend with when our refrigerators, cars and scores of other gadgets are all internet enabled and accessible through the internet!!

### **Ranganath Iyengar**

Managing Partner,  
Strategic Interventions India Pvt Ltd