**Cybercrime Cybercrime Everywhere- no place to hide**

**BY**

**PAVAN DUGGAL**

**ADVOCATE, SUPREME COURT OF INDIA**

**PRESIDENT, CYBERLAWS.NET**

**HEAD, PAVAN DUGGAL ASSOCIATES, ADVOCATES**

Globally, the year 2014 was a year that was dedicated to hacking and cybercrimes. In fact, cybercrime as a phenomenon loomed large and predominant on the firmament of cyberspace landscape. Looking at the predominant events that happened in 2014 across the world, one gets an intrinsic feeling that the year 2014 was a year to remind the world that cyber criminal activities and breaches of cybercrime are going to be an integral part of our day-to-day lives. Seen from another perspective, the predominant existing landscape also demonstrates an ongoing struggle between the digital haves and the digital have-nots. The world saw one of the biggest hacking attacks in the form of Sony hacking. In the said case, hackers reportedly infiltrated the computer network of Sony Pictures Entertainment, a major Hollywood movie studio. The attackers apparently stole a huge number of confidential documents, which are now being downloaded (primarily by journalists) from file-sharing networks. This event led to political events and war of words between the US and North Korea.

This was the year where projections concerning Cybercrime propagation and its frequency touched the roof top. As per latest projections, in 2014, it was projected that global losses connected to “personal information” breaches are estimated to reach USD 160 billion. Forty million people in the U.S., roughly 15 percent of the population, have had their personal information stolen by hackers. One study conducted by the Center for Strategic and International Studies (CSIS) tracked high-profile breaches around the world: 54 million in Turkey; 20 million in Korea; 16 million in Germany; 8.5 billion in Italy and more than 20 million in China and number of cybercrimes costs nearly USD 445 billion quantum worldwide.

2014 was also the year of the Home Depot hacking. An attack that led to the compromise of 56 million credit-card accounts and stealing of around 53 million customer email addresses.

2014 was the year when the Heartbleed virus was discovered. Heartbleed is a security bug in the OpenSSL cryptography library, which is a widely used implementation of the Transport Layer Security (TLS) protocol. Malware, spyware and spam continued to predominate in the year 2014. New kinds of virii came to be disseminated the world and more cybercrime activities loomed large.

The year 2014 was also remarkable for the iCloud hacking whereby nude photographs of various celebrities were hacked and put up onto the Internet. The year was full of important hacking attacks which were targeted at different computer systems and resources located in different parts of the world. Turkey saw a major hacking which involved a Turkish hacker group called RedHack attacking the systems of the Turkey Electricity Company and claiming to have deleted $796 billion of electricity bills of Turkish citizens in protest about the Turkish government’s censorship of the internet. The Gmail hacking in the month of September, 2014 led to 5 million Gmail usernames and passwords being compromised and about 100,000 were released on a Russian forum site. The year 2014 saw the eBay hacking which led to cyber attacks in late February and early March leading to the compromise of eBay employee log-ins, allowing access to the contact and log-in information for 233 million eBay customers. This led eBay to issue a statement asking all users to change their passwords. The year 2014 also saw the Russian hacking which led to Russian hackers stealing 1.2 billion user names and passwords in a series of Internet heists affecting 420,000 websites. The messages in 2014 were loud and clear that no computer system or network in the world was safe and the cyber criminals and cyber terrorists were increasingly targeting computer networks across the world for various political, vested and ideological purposes.

Bitcoins movement received a jolt when Mt Gox Bitcoins exchange collapsed due to malicious trading of Bitcoins. This was also the year when internationally the governments of the world continued to be living in an atmosphere of distrust and mistrust. Post-Snowden revelations, governments of the world were extremely concerned about potential interception, monitoring and surveillance happening or impacting their computer systems or networks as also resources. No major movement took place across the world in terms of concluding with any international dialogue or treaty towards protection and preservation of cyber security. The International Conference on Cyberlaw, Cybercrime & Cyber Security took place in November 2014 in India highlighted the significant issues impacting the intersection of Cyberlaw, Cybercrime and Cybersecurity and came up with various recommendations for international stakeholders. The year 2014 once again underlined the inefficacy of cyber legal regimes across the world to deal with emerging kinds of cyber challenges.

The year 2014 was also the year of the emergence of the dark web. This was the year when dark web started emerging and where Cybercrime as an economy model available in the dark web came to the forefront. This was also the year when the FBI was successful in shutting down Silk Road 2.0 after shutting down Silk Road 1.0 in late 2013.

This year also demonstrated how cyber legal regimes across the world are likely to face immense problems in terms of getting convictions done in cybercrime matters given the transnational nature of cybercrimes and given the transnational nature of the incriminating electronic evidence that has to be collected from different centers.

The author Pavan Duggal, Advocate, Supreme Court of India is Asia’s leading expert and authority on Cyberlaw. He can be contacted at his email addresses pavan@pavanduggal.com and pduggal@gmail.com. More about the Author is available at [www.pavanduggal.com](http://www.pavanduggal.com) and <http://www.linkedin.com/in/pavanduggal>.