DATAQUEST

Home   News   Features   Interview   Annuals   Case Study   Whitepaper   Opinion   Slide Show   Insights

Data Center

Cloud   DECEMBER 18, 2014

Small Company, Big Strides: How Tyrone Is Making Its Mark In HPC

It may seem that enterprise technology is a world that belongs to…

READ MORE   Share

HP delivers enterprise architecture for evolving business demands

0   -   NOVEMBER 6, 2014

Weekly Polls

How Is My Site?

- ○ Good
- ○ Excellent
- ○ Bad
- ○ Can Be Improved
- ○ No Comments

Vote   View Results

Subscribe to RSS Feeds

Send

Interview   AUTHOR: **ONKAR SHARMA**   -   NOVEMBER 5, 2014   Share   Twitter

No comments

IT Act 2000 lacks teeth

Ruchika Goel | dqindia

— Pavan Duggal

Cyber Law Expert and Advocate, Supreme Court of India

On the rise of cybercrime in India, Dataquest had a conversation with Pavan Duggal who is one of the top four cyber lawyers around the world. He is the President of Cyberlaws.Net and is working in the pioneering area of cyberlaw. While a practicing advocate, at the Supreme Court of India, Duggal has made an immense impact with an international reputation as an expert and authority on cyberlaw and e-commerce law. Excerpts

How would you explain cybercrime? In what forms is it flourishing?

Cybercrime has increased multifold in the last few years as more and more people have begun to use the Internet. Cybercriminals are after scapegoats and harnessing the weaknesses significantly. But there are different aspects of cybercrime. Basically cybercrime exists in three forms—Crime against property, crime against persons to defame or harass them, and crime against states or nations to wage cyber terrorism.

Is Indian law capable of handling the cybercrime instances which we often see occurring around?

Indian law lacks teeth to deal with cyber offenses. Ever since the Internet services were commercially launched in India on August 15, 1995, Indian law has not been able to deal with cybercrime. The existing I

Act 2000 and related sections of the IPC are not the distinct laws on cybercrime. Also, after the 2008 amendments in the IT Act, except for few cybercrimes, the rest have been made bailable. The law lacks strength to deal with cases.

Has the Indian law been able to set some examples through conviction in these cases?

This is an important point. Sadly, the IT Act is incapable of bringing offenders to justice. Till date there hav only been seven convictions in cybercrime cases. Because of the conviction rate being so low, offenders a getting the wrong impressions. It is important that cybercrime becomes non-bailable. Only then, India wil see decline in cases of this kind. At least there will be a fear.
Only crimes which are non-bailable are cyber terrorism, child pornography and breach of protected cyber system.

In the area of cyber warfare what trends do you see emerging post the NSA snooping became public?

The biggest cyberlaw trend in 2014 would be the enhanced frequency and instances of interception, surveillance, and monitoring across the world. The recent Snowden revelations regarding the US surveillance program PRISM have exhibited how networks and computer systems of legal entities outside a particular jurisdiction have been subjected to surveillance without the knowledge of such legal entities.

Many countries are likely to put in place stringent regulatory regimes which will aim to prevent/curb the unauthorized access to their network and further make such acts as penal offenses. However, the challenge will be to ensure as to how continued interception, monitoring and surveillance is to be regulate in a manner so as to give a semblance of respect to the rights and obligation to individual users of compute systems and digital ecosystem.

As technology will only erode the basic essentials of the concept of privacy in the digital ecosystem, what are the areas which will be critical for authorities to take care of?

The year 2014 is likely to see more calls to protect and preserve as also strengthen the legal regimes to help protect not just data privacy but also personal privacy of the relevant stakeholders.

The government needs to pay attention to build and implement policy so that cybercrime taking place in areas such as cloud, social media and mobility can be handled properly. For a country like India, it is important to take these thing seriously because if the law has teeth, it will send a positive message in the business community.

How prepared do you think our security and investigative agencies are to deal with cybercrime?

We need major capacity building in order to handle cases. At present security and investigative agencies are not able to deal with cybercrime. We need to train them with the latest technology so that they can think the way cyber criminals think. It will help in effective crime detection and investigation.

Posted by: **Onkar Sharma**

View more posts

 Facebook   Twitter   Google+   Linkedin   Pinterest

Related Posts