

## Insider attacks up in Indian cos

*By R Raghavendra/TNN*

Bangalore: Call them disgruntled employees or a bunch of hackers who have cut lose, they are a definite concern among Indian enterprises.

A recent study by Frost & Sullivan found that deliberate insider attack is 40% higher in India than in other countries. India is on the lower end of the curve when it comes to advanced attacks. However, this number is a bigger worry than a worm or a virus.



The study was done across five major markets in Asia, including India, over five weeks. A hundred interviews were conducted in each country, especially with those firms with a size of 250 people or more.

Deliberate attacks, beyond a certain point, cannot be monitored or controlled. Since most employees have access to the organisation's network, it is practically impossible for anyone to stop them from unleashing hell. To counter this, Indian organisations are taking to fragmentation of their network based on the nature of work or projects.

In simple terms, imagine one firewall which is managing two VLAN (Virtual Local Area Network). For better understanding, this can be called as two teams of people working on separate projects. A security threat in one particular group would not affect another because they converse with one universal firewall which is responsible for the overall communication between different groups across organisations. Fragmenting is all about separating your network to keep them away from a trigger effect (read attack).

"This method of fragmentation is slowly being adopted in BPOs. In the long-term, we see more organisations taking to this method," says Vishak Raman, country manager-India, Fortinet.

Further, the study also says that owing to slower networks, Indian companies are also of the view that ordering bandwidth is the most feasible solution. "It is here that we found that 1 out of 3 companies are interested in optimisation solutions," said Nitin Acharekar of F&S.

If 2005 saw desktop anti virus topping the rank of solutions adopted, this year would witness a strong interest in securing the network. In short, time and money would go into optimisation and security of the existing network.

The study puts India on the scanner and points out that almost 50% of respondents who are in support of outsourcing, plan to outsource their security needs. "Indian IT managers are expecting a higher increase in risk attacks in comparison to the average of countries studied. The risks could be in the form of virus and worms, phishing, hacking, deliberate insider as well as non-deliberate insider attacks," added Acharekar.

Indian companies spend 6-8% of their revenues on IT. Of this, about 7.8% goes on security while 6-8% is pumped into network. The rising interest to secure their network could see this numbers increase, besides the inclination to outsource.