CAT: glitches did us in, say candidates

Staff Reporter

BANGALORE: Even though the CAT 2009 was free of any major problem on the eighth day, candidates, who appeared for the test earlier under a "disturbed" atmosphere when technical glitches were encountered, are a worried lot now.

They are feeling that their performance would have been better if there had been no problems.

Ajay Arora, Regional Director, Triumphant Institute of Management Education, Bangalore, said that many candidates, who appeared for the computer-based test at testing labs which witnessed a series of problems, were disappointed.

He pointed out that those who completed the test under such conditions were the losers as they concentrated more on how the glitches could be overcome than on answering questions.

Rajesh and Pradhyuman said they were not happy with the environment at the testing lab. They said it was noisy, and many of the candidates panicked and were seeking the assistance of supervisors to overcome the technical problem. "A congenial environment is necessary when one writes any test; but unfortunately we did not have it," said Rajesh. Those who were unable to write the test were better placed than the others as their test had been rescheduled, they pointed out.

Meanwhile, there were rumours in the city on Saturday about cancellation of the test in some centres following a news report on a private television channel. However, Prometric, which is conducting the test for the Indian Institutes of Management, came out with an immediate clarification stating that tests had not been cancelled in any of the centres in the city.

(Names of candidates have been changed to protect their identity)

Online CAT fiasco turns the focus back on virus

Effective security solutions are a crucial line of defence for organisations

Shanthi Kannan

CHENNAI: The Common Admission Test (CAT) for admission to business schools went online for the first time this year. However, the experiment had a faulty start. Servers at 11 centres across the country crashed, as faults occurred unexpectedly as soon as the test began. It affected 12,000-odd aspirants, who appeared for the test on the first day of the examination.

Virus attack remains the major reason for the fault. Conflicker and W32.Nimda were named the principal culprits. Such viruses were reported way back in 2001. Nimda, which first appeared in September 2001, is a complex virus with a mass mailing worm component, which spreads itself in attachments named README.EXE. Like a number of predecessors, its payload appears to cause traffic slowdown.

Conflicker, also known as Conficker, Worm.Kido and Trojan.Kido, spreads among computers across a network by exploiting the vulnerability in the Windows server service (SVCHOST.EXE). It is also capable of spreading through removable drives and weak administrator passwords.

A virus attack caused servers at 11 centres to crash, leaving candidates tense on the first day of the Common Admission Test. – PHOTO: K. MURALI KUMAR

According to Shantanu Ghosh, vice-president, India Product Operations, Symantec Corporation, effective security solutions are a crucial line of defence for organisations to foil such attacks. Even if one computer on the network gets infected with a virus, all unprotected systems will suffer. These threats can also be spread through removable media such as CDs, pen drives and external hard disks.

One of the primary reasons why viruses infect networks is the absence of up-to-date security software. 'Free' software downloaded from the Internet can also be a threat, as it gives the user a false sense of security while being either ineffective in protecting computers or, even worse, downloading a malicious code, says Mr. Ghosh.

Mr. Ghosh says organisations should adopt a proactive, risk-based approach to security to ensure that infrastructure as well as information is protected. Deploying a data loss prevention solution, which can discover where confidential data is stored, monitor its usage, protect information, prevent its loss and manage and remediate security incidents, is crucial.

Data loss prevention solutions can monitor what enters and leaves the network to ensure that only those who have permission to access or modify data do so. Organisations also need to ensure that the variety of end-point devices that connect to the network — desktops, laptops, smartphones and removable media — is secure.