

Signs of maturity

Medium businesses are becoming seasoned veterans when it comes to deploying and managing security solutions, says *Abhinav Singh*

Medium businesses are aware of the importance of network security. While their adoption of security solutions does not compare with that of large enterprises, they are awakening to the fact that information security is essential. These companies have basic security systems in place. A third use anti-virus solutions. Firewalls, IDS and access control devices are also popular with some relying on encryption and cryptography. Integrated security appliances are occasionally used (AV, FW, IDS anti-spam in a box).

Vishak Raman, country manager-India and SAARC Fortinet, says, "Although medium enterprises' knowledge of security is not very high they are beginning to update their

security infrastructure. Going in for security certification is a sign of maturity."

Ajit Pillai, country manager-India and SAARC, WatchGuard Technologies, says, "About 33% of our business comes from the 100 to 500-user segment. Medium businesses are aware of the kind of security they want and they keep upgrading their security infrastructure. They do not want vendors to deliver point solutions. They prefer comprehensive solutions."

Telecom and IT/ITES sectors view security as a high priority area. For instance, Mumbai-based Zip Telecom manufactures pay phones and has chosen an integrated security appliance from WatchGuard. Nandu Bhat, general

manager IT, Zip Telecom says, "We were not able to scan e-mail for viruses and spam or detect and track network intrusion or where hacking occurred. With the integrated security appliance, many of these vulnerabilities have been plugged."

About 50% of medium business plan opt for a firewall, which is six points more than those who prefer anti-virus solutions. Intrusion detection systems (22%) and integrated security appliances (20%) are next in line. Investments have also been planned in encryption and cryptography tools, identity management and biometrics.

Most medium businesses have a documented security policy and are planning to in-



vest in network security. Of the verticals that were planning to invest in security infrastructure, manufacturing and engineering businesses lead, followed by the BFSI and the IT/ITES verticals. A high incidence of documented security policy reveals the maturity of security adoption in this segment.

The role of functional heads, CEOs and CIOs was critical in formulating security policy. Many medium businesses have an IT team headed by a CIO. The opinion of the functional heads and the CEO is considered while formulating security policy.

Data security is first among items on the security policy agenda followed by unautho-

rised employee access and data security in transit. Of the 71 businesses that have a documented security policy, 35 percent review it once a quarter. Another 22 percent review it once in six months and 28 percent once a year.

Around 15 percent also said that they had no fixed periodicity for reviewing security policies. The proportion of companies that review their security policy every three months is higher in auto and auto component manufacturers, telecom, IT/ITES and Government/PSU.

About 71% of respondents do not conduct security audits. And, 12% conduct internal audits, 9% choose ISO 17799 audits, 4% prefer COBIT and the remaining 4% are BS7799-certified. A security audit is a normal practice at 23% of those companies that do have audits. For 21% of these companies, it falls under the ambit of security policy. For the rest it either is a business or regulatory requirement, or because of client pressure. Frequency of audit varies from monthly, to two-, three- or six-monthly and annual. <