BUSINESSES are struggling to keep ahead of the large volume of attacks on IT systems and the ever-changing threats, the 2004 Australian Computer Crime and Security Survey shows.

Organisations are doing more to protect their networks, but about half were hit by attacks in the past year that harmed the confidentiality, integrity or availability of systems.

Electronic attacks and other computer crime cost public and private organisations an average $116,000 each — up 20 per cent on the previous year.

Respondents reported a total of $15.9 million in financial losses.

A whopping 88 per cent of attacks involved viruses, worms or Trojans, representing 45 per cent of total financial losses.

Of respondents surveyed, 60 per cent said attacks were successful largely because of unpatched or unprotected software — up from 29 per cent a year earlier — and 61 per cent said keeping up to date with threats was the hardest part of managing computer security.

They found it difficult to apply all critical patches to their systems in a timely manner.

Theft of laptops (58 per cent) and insider abuse of computer resources (69 per cent) were common problems.

The findings were greeted with concern yesterday at AusCERT2004, the Asia-Pacific IT Security conference held this week at the Gold Coast.

The survey, conducted by AusCERT in conjunction with law-enforcement agencies, canvassed large and medium organisations in 17 private industry sectors and local, state and federal government.

"Businesses are no longer sitting back in ignorance, but the environment is becoming more difficult to deal with," AusCERT director Graham Ingram said.

"People have been hit so often and so hard that dealing with these things should be an essential part of business.

"It's highly disturbing to find 60 per cent of attacks exploited common vulnerabilities."

Mr Ingram said early warning and preparation were key issues.

"We've got to stop the vulnerabilities that these worms exploit from being out there in such huge numbers," he said.

"That gets back to better software and better systems running on the internet."

The report's author, AusCERT's Kathryn Kerr, said worms and viruses did not discriminate; once released, writers had no way of knowing who would be hit.

People doing remote scanning were generally uninterested in their victims, but the machines they compromised could be used against others.
"An attacker's modus operandi is to compromise a third party's machine, whether it's a home user's ADSL broadband connection or a university's massive bandwidth link," Ms Kerr said.

"This minimises the chances of tracking back to the attacker."

Alastair MacGibbon, director of the AFP's High Tech Crime Centre, said criminals were constantly scanning the internet for vulnerable machines to hide behind.

"People might store their tools on one system and launch an attack from another," he said.

"You can turn up the compromised box but it's much harder to see where the traffic is coming from — to find who's controlling it.

"It's very rare that you can go straight to the offender, but there is a greater perception of anonymity than there is real anonymity. It's a matter of whether we are able to focus our resources."

Most attacks were launched from compromised boxes outside Australia, and the AFP routinely conducted inquiries offshore via its liaison network, he said.

"We're certainly seeing money flows offshore, particularly going into eastern Europe," Mr MacGibbon said.

"Because of the nature of electronic crime, though, that may not be the end-point for the money."

---

**THE FINDINGS**

Companies that are part of the nation's critical information infrastructure (CII) suffered more damage than those that were not. Half this sub-group reported harmful attacks, compared with 42 per cent of non-CII firms.

Most attacks came from external sources. "Unsolicited malicious damage" was cited by 52 per cent.

70 per cent of organisations reported higher spending on computer security in the past year, but only 5 per cent said they were managing all IT security issues well.

69 per cent said IT security staff lacked training and skills and 85 per cent thought general staff and management lacked awareness of security issues.

65 per cent said changing user attitudes and behaviour was a major challenge.

75 per cent said they had not reported harmful attacks to police or other authorities, compared with 62 per cent a year ago. Incidents were either considered not serious enough to report, or the organisation had not been explicitly targeted.

---

*Karen Dearne is attending AusCERT2004 as a guest of AusCERT*