

Gartner Says 60 Percent of Security Breach Incident Costs Incurred by Businesses Will Be Financially or Politically Motivated

Gartner Analysts to Discuss Defense in Cyberspace at Gartner IT Security Summit, June 2-4 in Washington, D.C.

STAMFORD, CONN., May 29, 2003 — By 2005, 60 percent of security breach incident costs incurred by businesses will be financially or politically motivated, according to Gartner, Inc. (NYSE: IT and ITB). Most of these financial losses will be the work of insiders working alone or in conspiracy with outsiders.

"Security managers and CIOs are well aware of the threat posed by insiders, but often find it easier technically and politically to take action against external threats instead," said Victor S. Wheatman, managing vice president for Gartner. "Businesses must take steps to secure themselves against criminally intent insiders or resign themselves to suffering significant losses from insider crimes."

Key modern business practices such as collaboration and knowledge management demand intensive information sharing, even across businesses. This open access often results in unauthorized use of computers and networks.

"There is a delicate balance between limiting insider access to information and crippling the ability to create revenue," said Richard Hunter, vice president for Gartner. "Generally, this conflict between security and commerce is resolved in favor of creating revenue and therefore facilitating insider crime."

Gartner advises that among other actions, businesses must create and enforce legal agreements defining legitimate use of proprietary intellectual property by trading partners and employees.

"Most businesses don't have procedures for establishing and enforcing agreements on shared use of intellectual property," said Wheatman. "Without such legal agreements, misuse is more likely and less subject to recovery."

Gartner analysts will provide further information on securing businesses against internal and external threats at Gartner IT Security Summit, June 2-4, 2003, in Washington, D.C., at the Washington Hilton.

The three-day summit will explore critical issues, best practices and case studies through panel discussions with top experts from the private and public sectors. Also included will be breakout sessions tailored to the critical infrastructure sectors such as transportation; energy, utilities and water; banking and financial services; telecommunications and information services; and vital health, safety and emergency services