



Cisco Contact:	Analyst Relations Contact:	Investor Relations Contact:
Perveen Akhtar	Henriette Borch	Roberta De Tata
Cisco Systems	Cisco Systems	Cisco Systems
+44 (0) 20 8824 4478	+44 (0) 20 8824 8603	+1 (0) 408 527 6388
pakhtar@cisco.com	hborch@cisco.com	rdetata@cisco.com

New Industry Research Reveals Businesses Spend More On Printers Than Network Security

IDC calls for security to be put on the boardroom agenda

LONDON, UK, April 27, 2004 – IDC today revealed that businesses are not taking the potentially devastating effects of viruses, worms and other breaches of security seriously enough. This is reflected in the amount of money that is invested in security solutions - \$42 billion in 2003. The figure is less than five per cent of the total IT spend - and is comparable to the \$43 billion annual spend on printers and multifunctional peripherals during 2003.

According to the research commissioned by Cisco Systems, human error and the time taken to maintain a network between attacks is what makes a business most vulnerable. The research also highlights key security issues which should be at the forefront of business leaders’ minds and calls for security to be a boardroom concern.

Thomas Raschke, Program Manager, European Internet Security at IDC said: “2003 was characterised by a tidal wave of viruses and worms. It therefore seems incongruous that spend on IT security is equal to that of the total spend on printers. Companies have to ask themselves what impact losing business-critical data will have. Those companies without the essential means of defence will be only too painfully aware.”

The blending of multiple attack types means that a security solution needs to be multilayered and holistic. According to IDC, antivirus software is not enough to protect a network and the data contained within it. “Viruses, worms, and other security breaches are evolving all the time, and there is an increasingly short period of time between identification of an attack and the time available for the software vendors to produce a suitable patch”, commented Raschke.

Another consideration that businesses must account for is the security of its outbound information, the validity and accuracy of which is critical to business operations.

“As sources of security attacks increase, there will be no let up in criminal ingenuity, carelessness of some staff or the impact of new regulations,” continued Raschke. “Whatever the case, breaches of security impact businesses in lost productivity, financial losses, regulatory compliance and shareholder value. Boardroom ownership of security and its implications is therefore mandatory. Attacks on businesses are not isolated, but part of sophisticated multilayered collaboration in order to circumvent point security solutions.”

The research points to the need for UK businesses to embed security into their networks so as to greatly reduce the threat of breaches that will result in network downtime.

“At IDC we predict that the total spend on security technology worldwide will exceed \$48 billion in 2004,” said Raschke. He predicts that the security market is estimated to increase from 4.8 per cent to 7 per cent of the overall IT budget by 2007.

IDC also predicts that the mobile security software market, driven primarily by the demand for remote access, will grow at a faster rate than the security market as a whole.

Cisco Systems' Senior Security Consultant, Paul King comments: "The Self Defending Network maximizes effectiveness in that the solution is designed to work from 'day zero' of an attack and is autonomic, therefore reducing the risk of human error."

King continues: "Businesses must also consider their remote workforce. It is critical that these networks are protected. Wireless networks are now hubs on the business network, and mobile phones and handhelds are an ever increasing target for virus writers."

IDC predicts that the mobile security software market, driven primarily by the demand for remote access, will grow at a faster rate than the whole security market. Security software solutions designed for the mobile and wireless environments are forecast to grow at a compound annual growth rate of 71 per cent, representing a \$1.27 billion market worldwide by 2007.

Other key points highlighted in the IDC white paper, titled Security – Embedded in to the Heart of Your Business, are:

- IDC believes that it is imperative for organisations to minimise security breaches, and the resulting business impact, to adopt a holistic approach to securing their networks.
- IDC estimate that expired email/user accounts may be upwards of 60 percent of all accounts in corporate systems. This not only makes the enterprise more vulnerable to breaches of security, but also increases administration costs.
- IDC believes that spam can account for up to 80 per cent of all inbound Internet email, opening the enterprise up to an unwanted source of potential security breaches.
- The rate of change of security threats demands continuous management of upgrades to security solutions.
- Security best practice starts and ends at the network.

###

About Cisco Systems

Cisco Systems, Inc. (NASDAQ: CSCO) is the worldwide leader in networking for the Internet. Information on Cisco can be found at <http://www.cisco.com>. For ongoing news, please go to <http://newsroom.cisco.com>.

About IDC

IDC is the premier global market intelligence and advisory firm in the information technology and telecommunications industries. We analyze and predict technology trends so that our clients can make strategic, fact-based decisions on IT purchases and business strategy. Over 700 IDC analysts in 50 countries provide local expertise and insights on technology markets. Business executives and IT managers have relied for 40 years on our advice to make decisions that contribute to the success of their organizations.

IDC is a division of IDG, the world's leading technology media, research, and events company. Additional information can be found at www.idc.com