



Businesses Worldwide Plan to Increase Spending on Network Security Next Year By as Much as 20 Percent

Global research measures impact of compliance, wireless mobility initiatives, mobile employee behavior, hiring, and other business drivers on network security planning

SAN JOSE, Calif. - August 29, 2007 - Cisco® today released a set of results from an additional international study examining mobile workers' security behavior with regard to corporate security and its impact on businesses, revealing widespread plans to increase security spending by as much as 20 percent next year to protect expanding wireless networks and the growing numbers of mobile employees who access them.

The latest research builds on findings released earlier this month spotlighting the growing trend of mobile employees and how their security behavior can heighten risks for business' IT organizations as they connect to corporate networks and carry sensitive information outside office walls. While the previous findings involve more than 700 mobile employees in seven countries where wireless and mobility technologies are widely adopted, the additional findings released today reveal spending plans and business drivers for more than 700 IT decision makers who work in those same nations: the United States, United Kingdom, Germany, China, India, South Korea, and Singapore.

Ultimately, the global study (conducted this spring by InsightExpress, an independent market research firm) explores what's driving IT to invest more heavily in securing connected business infrastructures. Their plans are driven by various business trends, such as regulatory compliance and strategic mobility initiatives, as well as the greater risks associated with increased collaboration among customers, vendors and partners.

"Businesses today are boosting productivity and corporate agility by enabling more employees to connect to the corporate network via mobile technologies," said John N. Stewart, Cisco's chief security officer. "Employees' awareness and behaviors relating to mobile security are the crucial factors in protecting information and assets."

Many mobile users say they aren't always aware of security concerns, and their actions provide proof. Throughout the seven countries, many mobile employees say they access unauthorized wireless networks in public places and in their neighborhoods. Many say they don't encrypt data on their wireless devices or set passwords to prevent physical access to their information. And, inevitably, some mobile users lose their devices or suffer from theft.

With behavioral security implications as a backdrop, more than half of the IT decision makers surveyed (55 percent) do not believe that the frequency of threats will decline. As a result, three of every four IT decision makers (74 percent) said security spending will increase over the next fiscal year in an effort to accommodate growing wireless and mobility requirements. Almost half (46 percent) expect investments to increase by more than 10 percent, and almost one of every 10 (9 percent) expects spending to jump *20 percent or more*.

"These figures are significant, because a 20 percent increase in spending on security alone could represent hundreds of thousands to millions of dollars for mid-size and large enterprises," said Jeff Platon, vice president of security solutions for Cisco.

Aside from the ever-present nature of security threats and behavioral concerns of mobile employees, the research revealed business-related reasons why spending is increasing:

- **Regulatory Compliance:** Just over half of the IT respondents (51 percent) say compliance drives them to focus more on wireless security, especially in Asia, where most respondents in China (75 percent), India (65 percent), and Singapore (62 percent) all feature a significant majority.
- **Mobility Enablement:** Almost two-thirds (63 percent) of IT respondents say more employees are being enabled to work anywhere, anytime with laptops, smartphones, or both. Germany (74 percent) lead the pack, followed by China and India (69 percent), South Korea (66 percent), and the United States (58 percent).
- **Corporate Growth and Hiring:** More than half of the IT respondents (53 percent) said hiring is increasing, which naturally increases the number of employees who will become mobile and wirelessly connected. In five of the seven countries, well over a half of its IT respondents note this development: China (69 percent), the United Kingdom (64 percent), Singapore (63 percent), India (62 percent) and the United States (53 percent).
- **Capital Expense Loss and Theft:** Nine percent of the IT respondents say spending is increasing as a result of replacing lost or stolen devices, such as laptops, smartphones and PDAs, most of which carry sensitive personal and corporate information. The United States features the most alarming percentage: More than one in four (26 percent) U.S. respondents say spending is increasing for this reason.

"The research really provides an opportunity for IT to reassess its relationship with increasingly mobile user bases and consider new ways to minimize spending," said Ben Gibson, Cisco's director of mobility solutions. "If you look at it from all angles - compliance, policies, business needs, and human behavior - technology is only half of the equation. Proactive communication, education, and engagement of employees on safe, appropriate online behavior, especially when they are mobile and remote, can help ensure solid returns on strategic IT investments that bring the promise of a secure, mobile wireless business to life."

About Cisco

Cisco, (NASDAQ: CSCO), is the worldwide leader in networking that transforms how people connect, communicate and collaborate. Information about Cisco can be found at <http://www.cisco.com>. For ongoing news, please go to <http://newsroom.cisco.com>.

###

Cisco, the Cisco logo and Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. This document is Cisco Public Information.

Contact Information:

Press Contact(s)

Neil Becker Cisco Systems, Inc. 408 525-7415 nebecker@cisco.com