

Cisco France

Véronique Jaffro – vejaffro@cisco.com
Tel : 01 58 04 31 90

Hill & Knowlton

Anne-Gaël Girard – anne-gael.girard@hillandknowlton.com
Tel : 01 41 05 44 48 / 29

62 % des professionnels IT souhaitent augmenter leurs dépenses de sécurité informatique en 2008

- Pour réaliser cette étude internationale commanditée par Cisco, InsightExpress a interrogé plus de 2 000 travailleurs nomades et professionnels des nouvelles technologies dans 10 pays : Etats-Unis, Royaume Unis, France, Allemagne, Italie, Japon, Chine, Inde Australie et Brésil.
- En 2008, la hausse de l'investissement sécuritaire sera même supérieure à 10 % pour la moitié des sondés souhaitant augmenter leur dépense dans ce secteur.
- Les pays les plus vulnérables face aux attaques informatiques, la Chine, l'Inde et le Brésil, sont également ceux qui souhaitent investir le plus en 2008.
- Leur vulnérabilité plus grande s'explique principalement par leur plus jeune expérience des risques encourus sur Internet, notamment lors de l'ouverture de mails non sécurisés ou de la connexion à des réseaux WiFi non sécurisés, en raison de la démocratisation plus récente de l'informatique dans ces pays.

#####

Cisco Study Reveals 3 of Every 5 IT Pros to Increase Security Spending in 2008

Global research explores implications of unchecked remote workers' security perceptions and behavior, creating opportunity for better education, smarter spending

SAN JOSE, CA - March 10, 2008 - Cisco today announced a final set of findings from annual research on remote workers' impact on corporate security, revealing that three of every five IT decision makers plan to increase security spending within the next year.

Commissioned by Cisco and conducted by InsightExpress, a third-party market research firm, the study features surveys of more than 2,000 remote workers and IT professionals from various industries in 10 countries: the United States, United Kingdom, France, Germany, Italy, Japan, China, India, Australia, and Brazil. While the first set of results released last month center on remote workers' security perceptions, online behavior, and their rationale for risky actions, today's findings focus on the implications that employees have on IT, and particularly the resulting financial burden. Sixty-two percent of the IT respondents reported that they will increase spending in 2008, and of those, more than half (37 percent) said their increased security investments will rise by more than 10 percent as compared to their previous years' budgets.

Global Demographics' Influence on the Behavior-Spending Connection

The findings indicate that spending will increase based on the financial losses that businesses suffer from attacks on corporate networks and employees - including employees who work outside of the office. One of the most intriguing findings involves global demographics, which play a significant role in worldwide security spending trends. The highest percentage of IT decision makers who plan to boost spending are from nations that are relative newcomers to widespread Internet and IP-based corporate networking. Of the 10 countries in the study, China, India, and Brazil feature the highest number of IT decision makers who are not only planning to increase spending in general, but the largest percentage who will increase security investments by more than 10 percent year-over-year.

According to John N. Stewart, Cisco's chief security officer, large populations of network-dependent employees in China, India, and Brazil were not overwhelmed by Code Red, NIMDA, and the other notorious malware attacks as pervasively as in Internet-dependent, consumer-based economies like the United States, United Kingdom, France, Germany, and Japan. However, today they represent three of the world's fastest growing economies, and their dependence on the Internet and corporate networks is rising rapidly. The study indicates that risky behavior from remote workers in these three countries, such as opening suspicious emails, hijacking wireless networks from neighbors, or sharing corporate devices with non-employees, is much more extensive than in nations that feature a longer history of corporate Internet use.

"During the past few years, virus attacks caused the most damage in countries where Internet adoption was greatest," Stewart said. "As new countries increase adoption, those that drive the new Internet growth can learn from others to understand the inherent security challenges - especially those who use the Internet to shop or work remotely. Remote workers often represent the intersection of 'employee' and 'consumer,' a connection point where attacks target and exploit the networks and corporate devices that remote workers use away from their offices. For multinational corporations and the IT departments that support them, understanding their employee's level of security awareness and experience is key in fostering tighter relationships, building trust, and administering effective education programs that will ultimately help to protect the enterprise."

Although China, India, and Brazil grabbed the spotlight, the spending trend is not relegated to emerging economies. More than half of the IT respondents in eight of the 10 countries are planning to increase security spending this year.

Total: 62 percent (37 percent to increase spending more than 10 percent)

- **India:** 83 percent (60 percent to increase spending more than 10 percent)
- **China:** 83 percent (58 percent to increase spending more than 10 percent)
- **Brazil:** 68 percent (56 percent to increase spending more than 10 percent)
- **Germany:** 61 percent (31 percent to increase spending more than 10 percent)
- **Italy:** 60 percent (35 percent to increase spending more than 10 percent)
- **U.K.:** 58 percent (29 percent to increase spending more than 10 percent)
- **Australia:** 55 percent (30 percent to increase spending more than 10 percent)
- **U.S.:** 53 percent (27 percent to increase spending more than 10 percent)
- **France:** 49 percent (22 percent to increase spending more than 10 percent)
- **Japan:** 24 percent (15 percent to increase spending more than 10 percent)

Putting It in Perspective: The Difference Between "Good" And "Bad" Spending

Security is a real-life business requirement, and Stewart affirms that the research provides global intelligence for IT organizations to take a practical approach to protecting their companies and employees, especially as they become more distributed. Just as IT budgets are a necessity, so too is security spending. What's important, he said, is to understand the delineation between what's considered "acceptable" and "unacceptable" spending. The goal is to prevent spending on reactive security "firefighting".

"Businesses need firewalls, virtual private networks, and data protection technologies," Stewart adds. "The challenge is how to minimize other costs that could have been prevented through sustained education of employees, such as managing malware outbreaks and data theft. Awareness, as the most effective tool, is not new thinking; the new thinking is how IT is leading the combined people, process, and technology to protect the enterprise most effectively. Increasing employee awareness through sustained education reduces threats, attacks, and the painful pricetags they typically carry."

The study's key findings will be spotlighted by Stewart and other security experts as part of a live Internet TV broadcast today from 8 a.m. to 9 a.m. PST on ways for businesses to protect their employees, assets, and bottom lines (to attend: <http://tools.cisco.com/cmn/jsp/index.jsp?id=70349>).

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.