INFORMATION PRESSE

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

Mobilité en entreprise : accroitre la vigilance pour une plus grande sécurité

- 2ème édition de l'étude annuelle conduite par InsightExpress dans 10 pays dont la France.
- 1 travailleur sur 2 a conscience d'être plus vulnérable en dehors de l'entreprise mais adopte malgré tout un comportement moins vigilant dans l'utilisation de son outil informatique. Ce phénomène est en croissance de 8 % par rapport à l'étude précédente.
- Plus d'un responsable informatique sur 2 estime que leurs collaborateurs sont peu disciplinés dans leur comportement en ligne. En croissance de 11 %, cela renforce aussi la nécessité d'informer sur les nouvelles menaces.
- En un an, l'augmentation de l'utilisation des outils de l'entreprise dans un cadre personnel (achats en ligne, téléchargement, réseaux sociaux, etc.) s'est nettement accrue, notamment en France et le taux est passé de 27 à 50 %.
- Pour lutter contre ces comportements à risques, l'étude propose des solutions pour permettre de réévaluer la perception des collaborateurs, et les conduire à un changement de comportement.

#####

Cisco Study on Remote Workers Reveals Need for Greater Diligence Toward Security

Global Research Spotlights Threat Landscape's Covert Evolution as Potential Reason for Softening Perceptions and Discipline Around Safe Online Behavior; Spurs IT Call to Action

SAN JOSE, Calif. - February 5, 2008 - Cisco® today announced key findings from its annual global study on remote workers' security awareness and online behavior, indicating how they can inadvertently heighten risks for themselves and the companies they work for. The study's findings are prompting Cisco security executives to offer recommendations to information technology (IT) professionals on how to protect their companies against threats and maximize the business benefits of distributed and mobile workforces.

Conducted by InsightExpress, a U.S.-based market research firm, the study involves surveys of more than 2,000 remote workers and IT professionals from various industries and company

sizes in 10 countries: the United States, United Kingdom, France, Germany, Italy, Japan, China, India, Australia, and Brazil. The 10 countries were chosen because they represent a diverse set of social and business cultures, stable and emerging network-dependent economies and varied lengths of Internet adoption.

The study's significance takes on growing importance as the number of remote workers increases worldwide. According to a 2007 Gartner report, "The worldwide corporate teleworking population of individuals that spend at least one day a month teleworking from home is expected to show a compound annual growth rate (CAGR) of 4.3 percent between 2007 and 2011. … In the same period, the worldwide corporate teleworking population of individuals that spend at least one day a week teleworking from home is expected to show a CAGR of 4.4 percent. This population will likely reach 46.6 million by the end of 2011."[1]

"Remote access and distributed workforces are here to stay. They provide competitive advantages and greater operational efficiency," said John N. Stewart, Cisco's chief security officer. "Businesses have the opportunity to benefit from productivity increases while preventing security risks from undermining them. This study provides intelligence and recommendations for understanding and minimizing risks as businesses allow employees to branch out beyond the traditional office. It explores their remote workers' psyche and provides valuable information about their approach to security."

A False Sense of Comfort?

One of the key findings is that remote workers feel less urgency to be vigilant in their online behavior. Although the majority believes they are more vulnerable outside the office than in, their perceptions of security threats are softening. In just one year, the number of remote workers who believe the Internet is safer increased 8 percent, from just under half (48 percent) to more than half (56 percent). This trend is especially prevalent in Brazil (71 percent), India (68 percent) and China (64 percent), three of the world's fastest-growing economies whose workforces depending more and more on the Internet and corporate networks.

According to the study, IT respondents believe their remote employees are becoming less disciplined in their online behavior: More than half (55 percent) believe their remote workers are becoming less diligent toward security awareness, an 11 percentage point increase from the year before. This perception shift may be a result of the threat landscape's evolution from overt to covert attacks. According to the Computer Security Institute's 2007 computer crime and security report, the number of financially motivated attacks surpassed traditional malware attacks (including viruses, worms, and spyware), and for the first time in the survey's 12-year history, the average annual loss from fraudulent attacks surpassed damages from malware. Although today's threats are more dangerous because they sabotage personal identities in addition to corporate intelligence, their invisible nature creates a false sense of comfort among employees that can result in a loss of discipline around online behavior, particularly when they work remotely.

"While working at home, people tend to let their guard down more than they do at the office, so adhering to security policies doesn't always intuitively seem applicable or as necessary in the private confines of one's home," Stewart said. "The blurring of the lines between work and home, and between business lives and personal lives, presents a growing challenge for businesses seeking to capitalize on the productivity benefits of the remote workforce."

Some of the key findings and reasons for risky behavior in year two include:

- **Opening emails and attachments from unknown or suspicious sources:** Although it is one of the age-old security risks, many remote workers admit that they still open suspicious emails and attachments despite the potential for triggering malware attacks. China (62 percent) is the most egregious offender. But arguably more disturbing is a growing trend in entrenched Internet-adopter countries like the United Kingdom (48 percent), Japan (42 percent), Australia (34 percent) and the United States (27 percent). For example, in Japan, 14 percent admit they open both an unknown or suspicious email and any attachments.
- **Using work computers and devices for personal use:** A 3 percentage-point increase year-over-year shows that more remote workers use corporate devices for personal use, such as Internet shopping, downloading music, and visiting social networking sites. This trend occurs in eight of the 10 countries, and the highest year-to-year spike occurs in France (27 percent to 50 percent). In Brazil, this trend rose 16 percentage points despite an increasing number of respondents agreeing that this was unacceptable behavior (37 percent to 52 percent year-over-year).
  Reasons Offered: *"My company doesn't mind me doing so", "I'm alone and have spare time", "My boss isn't around", "My IT department will support me if something goes wrong".*
- **Allowing non-employees to borrow work computers and devices for personal use:** As employees work more from home, the likelihood increases that they will share corporate devices with non-employees (e.g. family, roommates) who are not educated by IT or held to a company's security policies. This trend is increasing. While China features the highest rate of "device sharing" for the year (39 percent), the United Kingdom (from 7 percent in 2006 to 22 percent in 2007) and France (from 15 percent to 26 percent) reveal steep year-over-year increases.
  Reasons Offered: *"I don't see anything wrong with it", "My company doesn't mind me doing so", "I don't think it increases security risks", "Co-workers do it".*
- **Hijacking wireless Internet connections from neighbors:** Globally, 12 percent of remote workers admit to accessing a neighbor's wireless connection, with threefold year-to-year increases in Japan (6 percent to 18 percent) and France's 10 percent year-to-year rise (5 percent to 15 percent) representing the fastest-growing rates. China (from 19 percent in 2006 to 26 percent in 2007) and the United Kingdom (from 6 percent to 11 percent) also feature significant increases.
  Reasons Offered: *"I needed it because I was in a bind", "It's more convenient than using my wireless connection", "I can't tell if I'm using my own or my neighbor's wireless connection", "My neighbor doesn't know, so it's OK".*
- **Accessing work files with personal, non-IT-protected devices:** Accessing corporate networks and files with devices that are not protected by an employee's IT team presents security risks to the company, its information and its employees. As the number of remote workers grows, the study reveals an annual rise (45 percent in 2006 to 49 percent in 2007) in this behavior. It's widespread in many countries, especially China (76 percent), the United States (55 percent), Brazil (52 percent) and France (48 percent).
  Reasons Offered: *"These devices are secure with antivirus and other content security software", "I regularly use these devices to access my network", "My IT department has said it's OK to do so".*

Strategic Recommendations for Protecting an Increasingly Distributed Workforce

According to Stewart, now more than ever, it is imperative for the IT department to reassess how it's perceived by employees and how it can proactively influence corporate security. IT often approaches security exclusively from a technology perspective, but the need for security awareness, education, and proactive, sustained communication is as fundamental as purchasing a firewall. Spearheading this consultative engagement with employees represents a prime opportunity for IT to reshape its image in the eyes of its users and maximize the return on technology investments. It provides a platform for IT to be viewed not as a cost center, but as a true business enabler. In doing this, the research's multicultural scope highlights the need for IT security leaders to apply "localized" engagement and communicate more targeted approaches for different parts of the world.

"What we've found in year two reinforces the need for IT to triangulate awareness, education, and communication between their teams, executives, and employees," Stewart said. "How you communicate and educate employees about essential security practices and policies will be different in Japan than in the United States. It will be different in China than in France. Security awareness and education requires an understanding of your audience's culture. You have to relate to them and earn their trust. Through trust comes respect and cooperation.

"This research stresses the point that managing corporate security is part technology, part process, part awareness, education and communication," Stewart added. "It's often more of a human challenge than a technical one. And because of that, IT has the duty to emerge from the traditional back office to become more proactively engaged and consultative with its user base. Simply put, now is the time for IT to become more strategic than ever."

The study and key findings will be spotlighted by Cisco security executives, including Stewart, as part of a live Internet TV broadcast today from 8 a.m. to 9 a.m. PST on global threat trends and managing the human side of security challenges (to attend: http://tools.cisco.com/cmn/jsp/index.jsp?id=70346).

[1] Gartner, Inc. "Dataquest Insight: Teleworking, The Quiet Revolution (2007 Update)" by Caroline Jones, May 14, 2007

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.

# # #