



INFORMATION PRESSE

Cisco France

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

Hill & Knowlton

Caroline Langlais – caroline.langlais@hillandknowlton.com
Tel : 01 41 05 44 48 / 23

Cisco met en évidence les pratiques des salariés pouvant faire courir des risques aux entreprises

- Les principaux risques identifiés viennent de l'installation d'applications non autorisées (70%), de l'utilisation d'un ordinateur professionnel à des fins personnelles (66%) et du partage d'informations avec des personnes extérieures à l'entreprise (44%).
- Ces données sont tirées d'un sondage réalisé par InsightExpress auprès de 2000 salariés répartis dans 10 pays.
- L'étude met également en évidence de fortes disparités entre les pays, démontrant l'importance de l'aspect culturel dans les comportements des utilisateurs.

#####

Cisco Research Reveals Common Data Loss Mistakes

Global study explores behavioral risks based on country, culture - from accessing unauthorized facilities and networks to intentionally leaking corporate information

SAN JOSE, Calif. - September 30, 2008 - Cisco® today announced findings from a new global security study that spotlights numerous risks taken by employees that can lead to one of the most prominent security concerns for businesses: the loss of corporate information. The study identifies common data leakage mistakes among workforces around the world and is based on surveys of more than 2,000 employees and information technology professionals in 10 countries. The findings show that behavioral risks of employees can vary by country and culture, creating opportunities for businesses to tailor risk management plans that prevent incidents locally while remaining global in scope.

Conducted by InsightExpress, a U.S.-based market research firm, the study was commissioned by Cisco to examine security and data leakage (www.cisco.com/go/dlp)

implications for businesses at a time when employee lifestyles and work environments are changing dramatically. As the reliance on centralized offices shifts to distributed business models and remote workforces, lines are blurring between work life and personal life. This operational shift for businesses and the lifestyle overlap for employees are driven in large part by the proliferation of collaborative devices and applications that are used for both purposes, including mobile phones, laptops, Web 2.0 applications, video and other social media.

This evolving business environment serves as a backdrop for the study, which surveyed 1,000 employees and 1,000 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 countries were chosen because they represent a diverse set of social and business cultures, established and emerging network-dependent economies and varied levels of Internet adoption.

"We conducted this research in order to understand behavior, not technology per se," said John N. Stewart, chief security officer of Cisco. "Security is ultimately rooted in users behavior, so businesses of all sizes and employees in all professions need to understand how behavior affects the risk and reality of data loss - and what that ultimately means for both the individual and enterprise. Understanding this can help strengthen relationships between IT and employees, tailor localized awareness and education programs, and better manage risk. Simply put, security practices can be more effective when all users realize what their actions result in."

Of the many behavioral findings, the 10 most noteworthy were:

- 1. Altering security settings on computers:** One of five employees altered security settings on work devices to bypass IT policy so they could access unauthorized Web sites. This was most common in emerging economies like China and India. When asked why, more than half (52 percent) said they simply wanted to access the site; a third said, "*it's no one's business*" which sites they access.
- 2. Use of unauthorized applications:** Seven of 10 IT professionals said employee access of unauthorized applications and Web sites (e.g. unsanctioned social media, music download software, online shopping venues) ultimately resulted in as many as half of their companies' data loss incidents. This belief was most common in countries like the United States (74 percent) and India (79 percent).
- 3. Unauthorized network/facility access:** In the past year, two of five IT pros dealt with employees accessing unauthorized parts of a network or facility. This was most prevalent in China, where almost two of three respondents encountered this issue. Of those who reported this issue globally, two-thirds encountered multiple incidents in the past year, and 14 percent encountered this issue monthly.
- 4. Sharing sensitive corporate information:** In a sign that corporate trade secrets aren't always secret, one of four employees (24 percent) admitted verbally

sharing sensitive information to non-employees, such as friends, family, or even strangers. When asked why, some of the most common answers included, "I needed to bounce an idea off someone", *"I needed to vent"*, and *"I did not see anything wrong with it."*

5. Sharing corporate devices: In a sign that data isn't always in the hands of the right people, almost half of the employees surveyed (44 percent) share work devices with others, such as non-employees, without supervision.

6. Blurring of work and personal devices, communications: Almost two of three employees admitted using work computers daily for personal use. Activities included music downloads, shopping, banking, blogging, participating in chat groups, and more. Half of the employees use personal email to reach customers and colleagues, but only 40 percent said this is authorized by IT.

7. Unprotected devices: At least one in three employees leave computers logged on and unlocked when they're away from their desk. These employees also tend to leave laptops on their desks overnight, sometimes without logging off, creating potential theft incidents and access to corporate and personal data.

8. Storing logins and passwords: One in five employees store system logins and passwords on their computer or write them down and leave them on their desk, in unlocked cabinets, or pasted on their computers. In some countries like China (28 percent), employees reported storing logins and passwords to personal financial accounts on their work devices, leaving their identity and finances at risk. The fact that some employees leave devices unattended magnifies this risk.

9. Losing portable storage devices: Almost one in four (22 percent) employees carry corporate data on portable storage devices outside of the office. This is most prevalent in China (41 percent) and presents risks when devices are lost or stolen.

10. Allowing "tailgating" and unsupervised roaming: More than one in five (22 percent) German employees allow non-employees to roam around offices unsupervised. The study average was 13 percent. And 18 percent have allowed unknown individuals to tailgate behind employees into corporate facilities.

"Businesses are enabling employees to become increasingly collaborative and mobile," Stewart said. "Without modern-day security technologies, policies, awareness and education, information is more vulnerable. Today, data is in transit, in use, within programs, stored on devices, and in places beyond the traditional business environment, such as at home, on the road, in cafes, on airplanes and trains. This trend is here to stay. To protect your data effectively, we need to start understanding the risk characteristics of business and then base technology, policy, and awareness and education plans on those factors."

Stewart said these behavioral findings can help companies structure employee education programs at a regional level and sculpt global risk management plans. He lists recommended practices for preventing data loss, including:

- **Know your data; Manage it well:** Know how/where it's stored, accessed, used.
- **Treat data as if it's your own - Protect it like it's your money:** Educate employees how data protection equates to money earned and money lost.
- **Institutionalize standards for safe conduct:** Determine global policy objectives and create localized education tailored to a country's culture and threat landscape.
- **Foster a culture of trust:** "Employees need to feel comfortable reporting incidents so IT can resolve problems faster," Stewart said.
- **Establish security awareness, education and training:** Think globally, but localize and tailor programs for regions based on threat landscape and culture.

"Data protection requires teamwork across the company. It's not just an IT job anymore," he said. Today, the study will be presented in more detail by Stewart and other Cisco executives during a live Internet TV broadcast with media and analysts from 8 a.m. to 9 a.m. PDT. To attend: <http://tools.cisco.com/cmn/jsp/index.jsp?id=76034>.

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.