



# NEWS RELEASE

**Cisco Press Contact:**

Ben Stricker  
Cisco  
408-527-3199  
[bstricke@cisco.com](mailto:bstricke@cisco.com)

**Industry Analyst Contact:**

Trevor Bratton  
Cisco  
949-331-4954  
[trbratto@cisco.com](mailto:trbratto@cisco.com)

**Investor Relations:**

Marilyn Mora  
Cisco  
408-527-7452  
[marilmor@cisco.com](mailto:marilmor@cisco.com)

## **Beg, Borrow or Steal? Young Professionals, College Students Admit They'll Go To Extreme Measures for Internet Access Despite IT Policies, Identity Theft Risks**

*Tendencies of World Workforce's Next Generation to Ignore Online Threats Poses Challenge To Personal, Corporate Security; Magnify Findings in [Cisco 2011 Annual Security Report](#)*

**SAN JOSE, Calif. – December 14, 2011** – Seven out of 10 young employees frequently ignore IT policies, and one in four is a victim of identity theft before the age of 30, according to a global study from Cisco announced today. The final set of findings from the three-part [Cisco Connected World Technology Report](#) reveals startling attitudes toward IT policies and growing security threats posed by the next generation of employees entering the workforce – a demographic that grew up with the Internet and has an increasingly on-demand lifestyle that mixes personal and business activity in the workplace.

The [Cisco Connected World Technology Report](#) is an international study that examines the next generation of workers' demands and behavior involving network access, mobile device freedom, social media, and work lifestyles. The findings are key in explaining how this next-generation workforce's behavior heightens personal and corporate risk amid a complex threat landscape, a correlation that is spotlighted in more depth in the Cisco 2011 Annual Security Report, also issued today.

The latest findings from the Cisco Connected World Technology Report reveal growing concerns for employers. The desire for on-demand access to information is so ingrained in the incoming generation of employees that many young professionals take extreme measures to access the Internet, even if it compromises their company or their own security. Such behavior includes secretly using neighbors' wireless connections, sitting in front of businesses to access free Wi-Fi networks, and borrowing other people's devices without supervision.

Considering that at least one of every three employees (36%) responded negatively when asked if they respect their IT departments, balancing IT policy compliance with young employees' desires for more flexible access to social media, devices, and remote access is testing the limits of traditional corporate cultures. At the same time, these employee demands are placing greater pressure on recruiters, hiring managers, IT departments, and corporate cultures to allow more flexibility in the hope the next wave of talent can provide an edge over competitors.

The findings will be presented by Cisco's chief information officer and chief security officer during a free Internet TV broadcast at [www.cisco.com/go/connectedreport](http://www.cisco.com/go/connectedreport).

### **Key Findings**

- The second annual Cisco Connected World Technology Report surveys more than 2,800 college students and young professionals in 14 countries that represent the largest or fastest growing



# NEWS RELEASE

economies. It was commissioned to understand how companies must balance business needs and risk management with the next generation of employees' technology expectations and behavior.

## ***Risky behavior's impact on identity theft rates***

- Perhaps as a direct result of loosening privacy boundaries, about one in four college students (24%) and employees (23%) experiences identity theft before the age of 30. When applied to a broader pool of people, two of five college students said they know of friends or family members who have experienced identity theft. The following findings provide insight into the frequency of identity theft among this generation.

## ***Security and online privacy***

- One in three (33%) college students globally does not mind sharing personal information online, believes privacy boundaries are loosening, or does not think about privacy, providing foreshadowing for how the next generation of the global workforce will address information online – perhaps for business as well as personal activities.

## ***Adhering to IT policies***

- Of those who were aware of IT policies, seven of every 10 (70%) employees worldwide admitted to breaking policy with varying regularity. Among many reasons, the most common was the belief that employees were not doing anything wrong (33%). One in five (22%) cited the need to access unauthorized programs and applications to get their job done, while 19% admitted the policies are not enforced. Some (18%) said they do not have time to think about policies when they are working, and others either said adhering to the policies is not convenient (16%), they forget to do so (15%), or their bosses aren't watching them (14%).
- Two of three (67%) respondents said IT policies need to be modified to address real-life demands for more work flexibility.
- Companies restrict many devices and social media applications. Of these, young employees said online gaming (37%) was the most commonly restricted application. Apple iPods (15%) were the most commonly restricted device.
- One in 10 (10%) employees globally said IT policies prohibit the use of iPads and tablets, signaling a growing challenge for IT teams as tablet popularity increases. Three of 10 employees (31%) said social networking sites like Facebook, Twitter, and YouTube were prohibited as well.
- Three of five employees (61%) believe they are not responsible for protecting information and devices, believing instead that IT and/or service providers are accountable.

## ***Risky behavior: 'Borrowing' wireless connections from neighbors and stores***

- In the old days, neighbors would ask for eggs or sugar. Now they are asking for Internet access. Almost one in four college students (23%) has asked a neighbor for access to a computer or the Internet, and almost one in five (19%) admitted accessing a neighbor's wireless connection without permission. About one in five college students globally (19%) admitted standing outside retail outlets to use free wireless connections. About one in 10 (9%) has asked to use a stranger's mobile phone. Overall, two of three employees worldwide (64%) said they had done at least one of these actions.

## ***Risky behavior: Unsupervised computer usage***



# NEWS RELEASE

- More than half of the employees surveyed globally (56%) said they have allowed others to use their computers without supervision – family, friends, coworkers, and even people they do not know.
- College students exhibited higher tendencies than young employees to engage in risky online behavior. More than four of five college students (86%) said they have allowed others to use their computer unsupervised, indicating that this behavior is only going to become more prevalent as the next generation of employees enters the workforce over the next few years.
- More than one in 10 college students (16%) admitted leaving personal belongings and devices unattended in public, while getting something to eat or drink at a café or going to the restroom.

## *The Cisco Annual Security Report and Key Findings*

The Cisco 2011 Annual Security Report highlights the most important security trends of the year and provides tips and guidance to keep enterprise technology environments more secure. The Cisco Connected World Technology Report magnifies the threats outlined in the security report.

- **Dramatic Decline in Spam Volume:** According to [Cisco Security Intelligence Operations](#) (SIO), spam volume dropped from more than 379 billion messages daily to about 124 billion messages daily between August 2010 and November 2011—levels not seen since 2007. In the month of September 2011, India had the highest percentage of spam volume (13.9 percent). Vietnam came in second with 8.0 percent and The Russian Federation took the third-place spot with 7.8 percent.
- **Cisco Global ARMS Race Index:** Cisco's Global Adversary Resource Market Share (ARMS) Race Index was designed to track the overall level of compromised resources worldwide and, over time, to provide a better picture of the online criminal community's rate of success at compromising enterprise and individual users. According to data collected for this year's index, the aggregate number that represents the level of compromised resources at the end of 2011 is 6.5, down slightly from the December 2010 level of 6.8. When the Cisco Global ARMS Race Index debuted in the Cisco 2009 Annual Security Report, the aggregate number was 7.2, which meant enterprise networks at the time were experiencing persistent infections, and consumer systems were infected at levels capable of producing consistent and alarming levels of service abuse.
- **The 2011 Cisco Cybercrime Showcase:** The third annual Cisco Cybercrime Showcase presents two awards for 2011 – one acknowledging the outstanding contributions of an organization in takedowns of some of the world's worst botnets (the "Good," Microsoft) and the other recognizing the growing influence of a loosely organized group of Black Hats associated with collaborative, international hacktivism (the "Bad," Anonymous).

## **Supporting Quotes:**

**Rebecca Jacoby, CIO, Cisco:** *"The role of IT in any business is to successfully bring together technology architectures and business architectures. As workforces become increasingly mobile, the shift in IT infrastructure means that security and policy are no longer an "add-on" but the highest priority. These findings indicate a real need for a thoughtful and strategic approach for the types of IT services offered while taking into consideration the established processes and culture of any organization to create stronger, trusted relationships between employees and IT departments."*

**John N. Stewart, chief security officer, Cisco:** *"The next-generation workforce is looking for more open access to information and social media. The findings outlined in the Cisco Connected World Technology*



# NEWS RELEASE

*Report provide valuable insights into how we must adapt IT and security policies to enable mobility and productivity while still managing risk. Done well, security enables mobility and social media access to provide the necessary productivity boost.”*

## Supporting Resources

- [Watch an overview](#) of Chapter 3 of the 2011 Cisco Connected World Technology Report’s findings, featuring an analysis by Cisco executives, including CIO Rebecca Jacoby, CSO John Stewart and VP of IT Lance Perry
- View the infographics for Chapter 3 of the Cisco Connected World Technology Report at [www.cisco.com/go/connectedreport](http://www.cisco.com/go/connectedreport)
- Review the findings from all chapters of the 2011 and 2010 Cisco Connected World Technology Reports, including previous press releases, metrics, infographics and Cisco TV broadcasts: [www.cisco.com/go/connectedreport](http://www.cisco.com/go/connectedreport)
- Read “Top Ten Findings from the 2011 Cisco Connected World Technology Report” on the [Borderless Networks](#) blog
- Download the [Cisco 2011 Annual Security Report](#)
- Follow [@CiscoSecurity](#)
- Visit Cisco [Borderless Networks](#) Web site

## About the Cisco Connected World Technology Report

- The Cisco Connected World Technology Report was commissioned by Cisco and conducted by InsightExpress, a third-party market research firm based in the United States.
- The global study focuses on two surveys – one centering on college students, the other on a group of young professionals in their 20s. Each survey included 100 respondents from each of the 14 countries, resulting in a survey pool of 2,800 people.
- The 14 countries were Australia, Brazil, Canada, China, France, Germany, India, Italy, Japan, Mexico, Russia, Spain, the United Kingdom and the United States.

**Tags/keywords:** Cisco, routing, switching, enterprise, security, wireless, mobility, Cisco Connected World Technology Report, survey, college, Millennials, newspapers, Twitter, Facebook, workforce, HR, BYOD, Bring Your Own Device, Wi-Fi, ScanSafe, access policy, TrustSec, secure mobility, network security, firewalls, controller, SecureX, spam, virus, malware, software-as-a-service, SaaS, security as a service, enterprise security, security appliance.

**RSS Feed for Cisco:** <http://newsroom.cisco.com/dlls/rss.html>

## 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>.



# NEWS RELEASE

# # #

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned 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.