White Paper

Understanding Remote Worker Security: A Survey of User Awareness vs. Behavior

EXECUTIVE SUMMARY

To study remote worker behavior, Cisco Systems® commissioned InsightExpress, a third-party market research firm, to survey end users from a variety of industries. The surveys were conducted in parallel in 10 countries: the United States, the United Kingdom, France, Germany, Italy, Japan, China, India, Australia, and Brazil. More than 1,000 remote workers were surveyed. The survey revealed that most remote workers believe they are working securely, yet they continue to engage in risky online behavior.

- **Online shopping:** Nearly 40 percent of remote workers in the same respondent pool said they use their work computers for Internet shopping. Half said they make personal online purchases because their "company does not mind them doing so."
- **Sharing computers:** 21 percent of users admitted that they allowed others to use their work computers. More than one in four stated that they "don't see anything wrong with it." And believed computer sharing "does not increase security risks."
- **Risky wireless behavior:** One in 10 users surveyed stated that they have used a neighbor's Internet connection when working remotely. Most stated they did so because "they were in a bind." 18 percent stated that "my neighbor doesn't know, so it is OK."
- **Personal devices:** Almost half reported that they used their own personal devices to access corporate resources. Yet only half of those who used these devices said they had antivirus or security software on the devices.
- **E-mail downloading:** 10 to 20 percent of users in India and Brazil admitted to opening unknown e-mail messages and their attachments. 38 percent of users reported that they click on unknown e-mail messages but do not open attachments.

Although remote workers understand the importance of security, their behavior suggests that IT should improve efforts to educate and collaborate with users. By actively encouraging two-way communication with end users, IT can take an important step toward a more comprehensive security strategy.

INTRODUCTION

In today's increasingly globalized business environment, organizations of all sizes are becoming more distributed. They rely more than ever on remote workers, and for good reason. A mobile workforce can respond to customers more quickly, be more productive and agile, and enjoy better job satisfaction. Whether it's a salesperson on the road, a doctor at home, or a PR manager in a coffee shop, organizations are enabling their employees to work anywhere, at any time, and in any way—all to generate competitive advantages and greater productivity.

Despite the benefits to businesses, a remote workforce poses security risks. Telecommuters use everything from notebook PCs to handheld PDAs to access their networks, and they frequently use wireless connections in public places. Wherever they go, they carry the access to their companies' data, not to mention their own personal information. Because they are working independently and outside of centralized, physically secure offices, teleworkers and mobile employees are vulnerable to network threats that are less common inside an office. What's more, remote workers are often the first to contend with new security threats and therefore are often the sources of network breaches. Even a single security incident involving a remote worker can ripple quickly throughout the rest of an organization.

Companies have placed their most-critical business processes on the network, and a breach in security can quickly escalate into lost time and money, compromised data, reduced productivity, or diminished customer confidence. Security for remote workers is critical not only for a company's day-to-day operations, but also for network resilience planning. As organizations become more aware of the need for disaster recovery strategies, they need to be especially cognizant of remote workers' behavior. Understanding exactly how remote

employees work is crucial for a company that might have large numbers of employees working remotely during a natural disaster, pandemic, or other network disruption.

As the stakes grow higher for network integrity, the threat landscape is rapidly evolving as well. More than ever, IT organizations require greater agility and knowledge about how to combat attacks before they become full-blown problems. Security challenges are growing in number and intensity, and seeping into every aspect of a business organization. Threats are becoming more complex, stealthy, and profit-motivated.

As security threats and concerns evolve, end-user behavior is changing. Working remotely is no longer the exception, but a way of life for many employees. To respond immediately to clients and colleagues, employees are becoming dependent on constant access to the network. They are used to responding to e-mail or accessing the company server at any time of day. Employees depend on the Internet for their everyday business activities, and face a broad array of tempting e-commerce sites, file sharing environments, and online communities that can pose security risks.

Users are also becoming more complacent. They believe that their IT organizations are responsible for protecting them, and as a result are most likely unaware of new or emerging security threats. To overcome these new challenges, IT organizations need in-depth insight into their users' attitudes and behavior. Armed with this knowledge, they can take steps to move their security strategies forward and proactively confront these emerging threats.

IN-DEPTH SURVEY REVEALS RISKY BEHAVIOR

To better understand how remote workers affect security risks and planning for IT, Cisco Systems commissioned InsightExpress, a third-party market research firm, to survey end users from a wide range of industries. The surveys were conducted in parallel in 10 countries: the United States, the United Kingdom, France, Germany, Italy, Japan, China, India, Australia, and Brazil. In each country, more than 100 remote workers were surveyed.

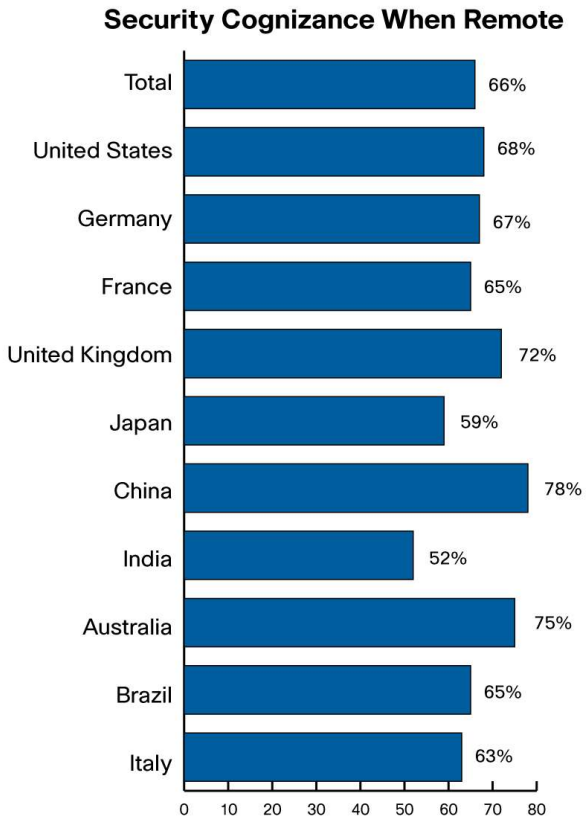
The survey results reveal a surprising set of end-user perceptions, experiences, and behaviors. These perceptions and behaviors heighten security risks for IT organizations in environments that lack perimeters, boundaries, or full corporate oversight.

For example, despite a high admission of security awareness and cognizance, telecommuters' work practices are not always consistent with this reported awareness. Many users regularly open unknown e-mail messages and attachments, connect to neighbors' wireless networks, share their work computers with non-employees, and engage in Internet shopping.

AWARENESS ALONE IS NOT ENOUGH

Awareness is a crucial first step in safeguarding organizations. The global survey indicates that the majority of remote workers (66 percent) are cognizant of security concerns (Figure 1).

Figure 1. End users significantly agree that they are more cognizant of security concerns when they work remotely.

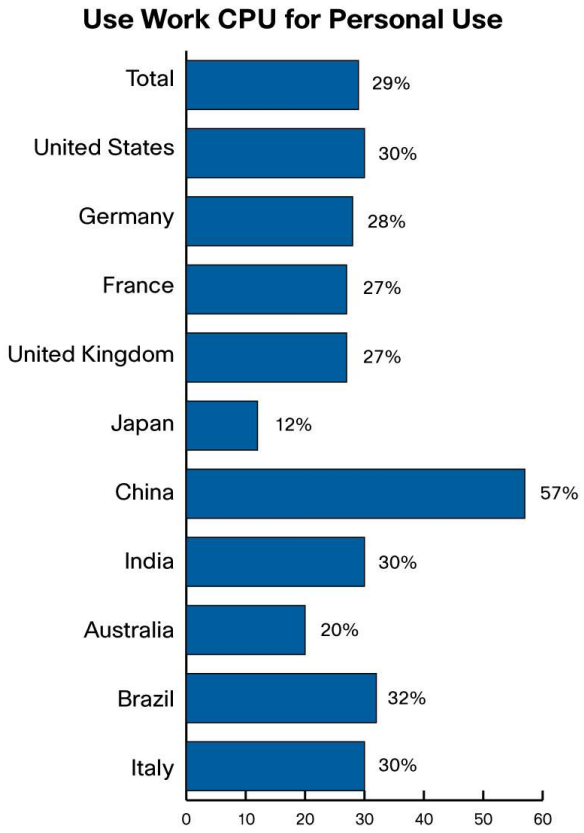


While end users might be aware of the importance of security, this knowledge is not enough to ensure safer behavioral habits among remote end users. Just because users think or say they are cognizant does not mean they know how to be safe. An end user who is poorly informed about security best practices, yet believes he is working safely, can actually exacerbate security risks for IT organizations.

To explore the relationship between user beliefs regarding security and their behavior, the survey included a series of specific questions on behavior. Perception played an important role in determining how end users actually behave when working remotely. The survey revealed that although many remote workers believe they are working securely, they continue to engage in risky online behavior.

For example, the survey showed that nearly one-third (29 percent) of users use the company computer for personal use (Figure 2). This belief not only affects productivity but also invites greater security threats.

Figure 2. Significant numbers of users surveyed reported using their employer's PC for personal use. In China, 57 percent of users engaged in this risky behavior.



HOW SAFE ARE USERS?

As the scope and intensity of security threats escalates, even seemingly harmless behavior by remote users can invite serious security breaches. Many end users admitted to engaging in risky online behavior when working remotely—from Internet shopping and opening suspicious e-mail messages to "hijacking" neighbors' wireless networks and sharing work computers with others. Most remote workers surveyed say they are aware of the need to use best practices and take precautions to protect their organizations from security threats, but their behavior tells another story.

Online Shopping

A considerable majority of survey respondents (71 percent) said they do not use work computers for personal use. Yet nearly 40 percent of remote workers in the same respondent pool said they use their work computers for Internet shopping.

When asked for additional details about their justification for online shopping while working remotely, end users offered a variety of explanations (Table 1).

Of those who admitted to online shopping on work computers:

- 49 percent stated they make personal online purchases because their "company does not mind them doing so."
- 43 percent said they "would never get personal things done if they did not do them at work."

Table 1. Most end users make personal online purchases because their "company does not mind them doing so" and they "would never get personal things done if they did not do them at work."

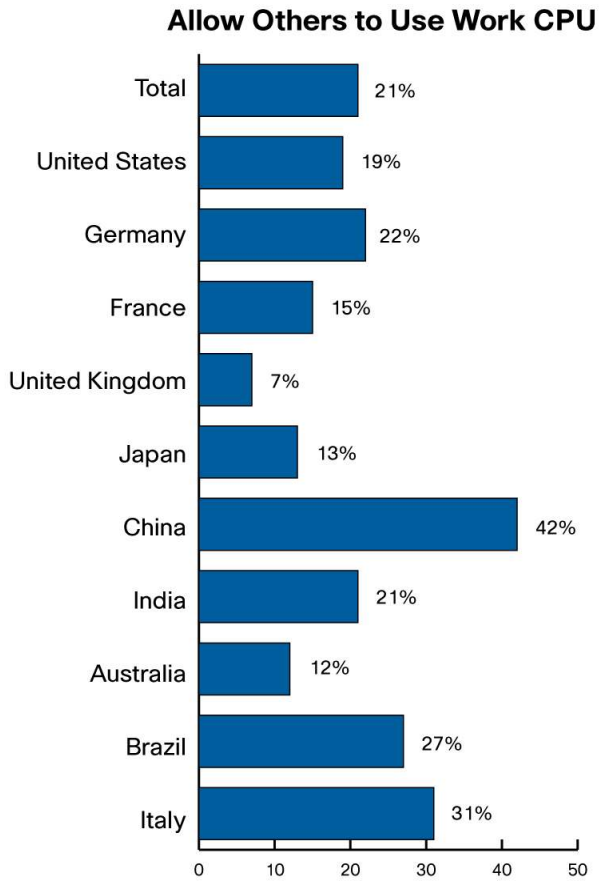
	Would never get personal things done if I didn't do them while at work	Shopping online can't result in security problems	I think my work computer is more secure than my home computer	It's OK as long as my boss doesn't see me	Other co-workers do it	My company doesn't mind me doing so	I doubt my company would care	I doubt my company would find out	IT department will support me if there's a problem
Total	**43%**	**22%**	**21%**	**9%**	**18%**	**49%**	**24%**	**7%**	**16%**

These responses suggest that users shop online for convenience, without closely evaluating whether or not their behavior is risky. The survey also reflected a lack of awareness about the risks associated with online purchases. In Germany, 26 percent believed that shopping online cannot result in security problems.

Sharing Work Computers and Devices

Sharing a company computer with a user outside the company can be an invitation to security problems. Outside users have not been educated by a company's IT organization, and are not beholden to its security policies. Nonetheless, the survey revealed that significant numbers of end users share their company computers with other users. Despite their awareness of the importance of security, 21 percent of users admitted that they allowed others to use their work computers (Figure 3). In fact, respondents in Japan said they allow others to use their computers for personal reasons more than they do themselves.

Figure 3. Significant numbers of end users allow others to use their company computers.



Ignorance about security risks and best practices appear to be driving this type of behavior as well.

- 37 percent of remote workers who shared their computers with others—whether family members or friends -- stated that they “don’t see anything wrong with it.” 26 percent believed computer sharing “does not increase security risks.”
- One of every three respondents (35 percent) who shared their computers said their “company does not mind my doing so,” suggesting that IT staff may want to revisit their own policies, or communicate them more effectively to end users.

Risky Wireless Behavior

Another surprising response came from users who exposed their computers and data to unsecured network connections. One in 10 users surveyed stated that they have used a neighbor’s Internet connection when working remotely. In China and Brazil, 20 percent of users engaged in this type of behavior.

Most end users who have “hijacked” their neighbors’ wireless connections have done so because “they were in a bind.” And 20 percent of participants stated that they “can’t tell if I’m using my own or someone else’s wireless Internet connection.” Another 18 percent stated that, “my neighbor doesn’t know, so it is OK.”

Like the Internet shoppers, this group seemed more concerned with expedience and saving time than with safety and courtesy toward neighbors. In China, half the teleworkers surveyed stated that using a neighbor’s wireless network was simply “more convenient” than using their own wired Internet connections.

Personal Devices

Personal devices that users connect to the network pose serious security risks for organizations. Oftentimes, these devices may not be governed by IT and security policies, or comply with best practices.

Some 45 percent of end users stated that they used their own personal devices to access corporate resources. In China, this number soared to 74 percent of end users. Yet only half of those who used these devices said they had antivirus or security software on the device.

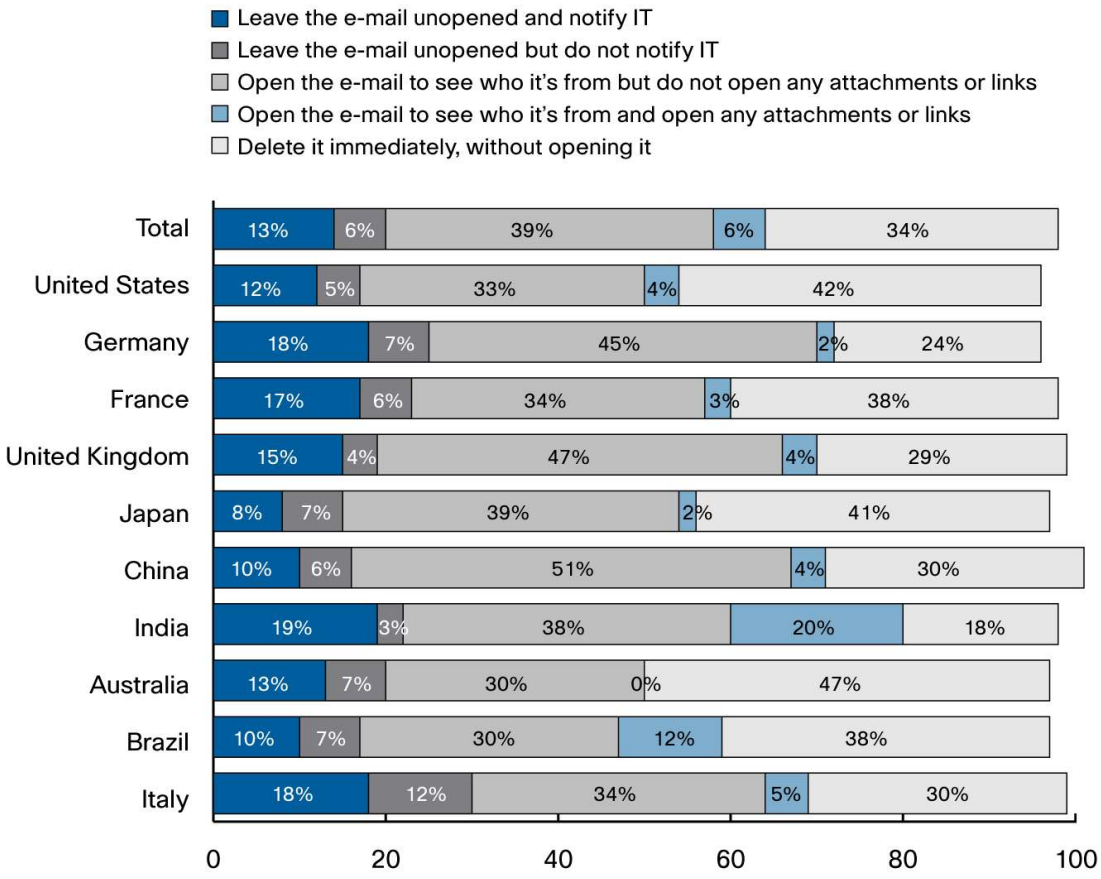
- 29 percent of users believed that access by personal devices was safe.
- 36 percent believed using personal devices for network access was acceptable simply because they did so regularly.

Downloading and E-Mail Behavior

Downloading files to the company network or to work devices has long been recognized as a particularly risky behavior. Viruses, Trojan horses, and other types of malicious files are well-publicized, and most corporate users are well aware of these threats.

Nonetheless, surprising numbers of users continue to open e-mail messages and attachments sent from unknown sources (Figure 4). Even a single instance of a user opening a virus or malicious file can cause a great deal of damage. Consider the impact of careless handling of e-mail and attachments by just 50 people in a 1000-person company. Large organizations with thousands of users cannot tolerate this behavior by even a small percentage of their users.

Figure 4. End users are not notifying IT when they receive unknown e-mail, but often open and delete it.



A sizable percentage of respondents (38 percent) reported that they click on unknown e-mail messages but do not open attachments. This activity is less risky than opening unknown files, but can still present security risks.

- In India and Brazil, 10 to 20 percent of users admitted to opening unknown e-mail messages and their attachments. These figures are alarming: even one bad file can wreak havoc on an organization.

Bringing one's own personal files into the secure business environment can cause problems as well, yet the survey results show that this type of behavior was common.

- 46 percent of end users download personal files to corporate networks or their work devices.
- In both China and Australia, more than 58 percent of participants port their own files to their work environment.

IT'S CHALLENGE—AND OPPORTUNITY

The contradictory relationship between many teleworkers' security awareness and behavior illustrates the challenge IT must face every day in safeguarding their companies. To promote effective security strategies, IT organizations must rethink and reassess their relationships with end users, to engage more proactively with their clients.

Traditionally, users have considered IT a monolithic service organization that simply addresses network problems after they happen. IT would react to user issues after the network went down or when computers were compromised.

As security threats become more sophisticated and pervasive, IT must make an extra effort to foster two-way communication with users. They need to make themselves known, establish their authority, and communicate best practices more effectively. At the same time, IT organizations must listen to their clients for better insight into how their users perceive security issues. Without an ongoing dialogue, IT will have only a limited view of how well teleworkers understand security and apply best practices when working remotely.

It's clear that end users understand the importance of security. Yet they are not IT professionals and cannot be expected to understand a rapidly changing threat landscape. They have different priorities. By collaborating with their end users and educating employees about risky behavior, IT can make major strides toward implementing sound security policies. At the same time, they can fine-tune their strategies for employing comprehensive, in-depth security technology. As they work to align their users' perceptions more closely with reality, IT organizations can help their businesses participate in promoting safe, secure workplaces.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco.com Website at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in USA C11-366486-00 10/06