White Paper

Cisco Connected World—International Mobile Security: *Survey Research Highlights and Considerations for Enterprise IT*

Executive Summary

To better understand the rising security challenges associated with integrating mobile devices into business operations, Cisco recently conducted an international survey that explored the attitudes and experiences of end users worldwide. The *Cisco Connected World—International Mobile Security* survey covered a range of topics, including:

- Employee attitudes toward using personally owned ("personal") and company-issued devices to access corporate networks
- The types of personal and company-issued devices used for network access
- Online behavior of employees using mobile devices
- Employee perceptions of mobile device security

As the number of mobile devices in the workplace continues to expand, IT organizations and the businesses they serve can use these insights to determine how best to approach providing their workers with productive, flexible, and secure network access from any device.

Introduction

Enterprise mobility and the "consumerization of IT"—employees' use of consumer devices and cloud applications in the enterprise—are well under way across the globe. But IT organizations, particularly those in large enterprises, are struggling to keep pace with and respond to the impact of these trends—namely, the deterioration of the traditional security perimeter, the proliferation of endpoints that must be secured, and the intensifying demand by workers for anytime, anywhere access to corporate assets using mobile devices that they choose.

IT administrators remain challenged in finding the optimal balance between securing sensitive corporate data and allowing employees to have access to the tools and information they need for productivity. Mobile devices are prone to loss and theft, which means so are the data and access credentials they hold. Employees using public networks to transfer data to mobile devices can put sensitive corporate information at risk. And users who access the Internet from their mobile devices are at constant risk of exposure to web-based threats, including data-stealing malware.

Finding balance is imperative, however, because it is more than just a matter of security. The evolution of integrating mobile device technology into business operations offers a platform for ongoing, cost-effective innovation that powers a more collaborative and productive workforce. In an increasingly connected world, embracing mobile technology will enable organizations to maintain their ability to not only compete, but also attract and retain top talent.

The *Cisco Connected World Technology Report*[1] initially examined changing attitudes toward work, technology, and security among college students and young professionals (emerging workforce or end users) around the globe. The *Cisco Connected World—International Mobile Security* survey expanded the research to the entire workforce and suggests that enterprises have yet to fully implement many basic security procedures for both mobile devices and remote access to corporate data. It is especially clear that organizations need to place greater emphasis on creating and enforcing policies that are robust, yet flexible, and educating users about potential threats and best practices for avoiding them.

Using Personal and Company-Issued Devices for Work

Findings for the *Cisco Connected World—International Mobile Security* survey show fairly equal numbers of respondents are using either employer-provided or personal laptops, desktop computers, smartphones, or tablets for their everyday job duties. Some use a combination of these devices.

The significance of these results, of course, is that using a personal device for work purposes is becoming increasingly commonplace. In fact, nearly half (45 percent) of respondents said their employer gives them a set budget to purchase their own laptop, smartphone, and other device of their choice, rather than provide everyone with the same equipment. Most employers also paid for the voice and/or data subscriptions for their employees' personal devices used at work.

More than half of all respondents said that company-issued devices should be available for personal use. And virtually all respondents said they believe it is at least somewhat important that they be able to access the same applications, desktop, and data, and have the same user experience, whether they are using a company-issued or personal device.

Considerations for IT:

- How can we protect applications and data on all devices?

Seamless Remote Access

Enterprises appear to be making some progress in supporting the growing population of mobile and remote workers, according to the *Cisco Connected World—International Mobile Security* survey. More than half of respondents report that they currently have the ability to connect seamlessly to their corporate network from anywhere at any time. Among the countries surveyed, respondents from Brazil, India, and the United States reported having the least amount of difficulty remotely accessing information from their corporate network. This could indicate that their employers have achieved secure connectivity for their remote and mobile workers; however, it could also mean the opposite.

Interestingly, while most survey respondents said they consider remote access a privilege, not a right, many still have high expectations about remote connectivity and lament the lack of seamless access provided by their employers. In particular, respondents from China—many of whom view remote access as a right—identified IT restrictions as their greatest frustration. Other respondents cited corporate policies, budget limitations, and industry regulations as top obstacles to seamless remote access.

Considerations for IT:

- How can we secure remote workers—and not compromise user experience?

[1] Cisco Connected World Technology Report, 2012: http://www.cisco.com/en/US/netsol/ns1120/index.html.

Secure Connections

While more employees are demanding to use their device of choice in the enterprise, many also recognize there is some risk for their employer in embracing the "bring your own device" (BYOD) trend. Most respondents believe an Internet-enabled personal smartphone poses a greater security risk than a company-issued smartphone.

Nearly half (46 percent) of respondents view a wired laptop connection as the most secure way of connecting remotely. However, the majority of those surveyed (60 percent) also said that when working remotely, they borrow someone else's wireless connection at least sometimes. (Of note: Half of respondents from India report borrowing others' connections "all the time.") Lack of access to another Internet connection and convenience were cited as the top two reasons for borrowing wireless connections.

Considerations for IT:

- How can we ensure secure remote access from wireless connections?
- How can we make sure our secure access efforts are consistent for users of both company-owned and personal devices?

Online Behaviors and Encounters with Threats

Results from the *Cisco Connected World—International Mobile Security* survey show that while most employees are aware of the risks that mobility presents to enterprise security, most still report engaging in risky behavior when using their mobile devices. In fact, 26 percent of respondents from the total survey sample said they take more risks with company-issued devices than their personal devices. The reason, according to those who reported being bolder with online behavior when using a company-issued device, is the belief that IT will provide support if something goes wrong. (This attitude likely includes the belief that current threat defense software will help to provide protection.) Examples of "risky" mobile device behavior include:

- **Use of collaborative applications:** Forty percent of respondents reported using collaborative applications such as voice, video, and web conferencing; messaging; mobile applications; and enterprise social software on the mobile devices they use for work. Often, collaborative applications are web-based, and IT either may not control their use or may be unaware that employees are using them. Respondents, particularly those in China, who do not use collaborative applications on their company or personally issued devices, tend to indicate security concerns as their main barrier.
- **Downloading sensitive corporate data onto a mobile device:** Most respondents (63 percent) said they download sensitive corporate data onto their personal computer or mobile device at least sometimes. This is more prevalent and frequent in some geographies, particularly in India, where most end users (58 percent) download sensitive corporate data "all the time." Across all countries represented in the survey, respondents who engage in this behavior said they do so because they "needed the information wherever I go—whether it's secure or not."
- **Not protecting data once downloaded to a mobile device:** About 10 percent of survey respondents reported that they do not take steps to protect data they download on their wireless mobile device. One reason for this behavior is clear—and is easily correctable through user education: Roughly half of those who said they never use encryption or set passwords on their wireless devices indicated they don't know how to do so.

Web threats were another significant security concern: Nearly half of workers surveyed said they had encountered issues with web threats such as viruses and phishing when using a company-issued device. Even larger proportions had encountered web threats when using a personal device. The threat of malicious downloads from the web appeared to be less common. Only one-third of respondents said they had experienced a malicious download on their company-issued or personal device.

As for security alerts: When they see a warning pop-up on either a company-issued or personal device, most respondents said they click through and read the details carefully before deciding how to proceed. (However, respondents in India and the United Kingdom seem to be generally less careful than workers from other countries surveyed in that they will accept warning pop-ups without reading the details.)

Considerations for IT:

- How can we enforce “good behavior” among employees using mobile devices?
- How can we protect enterprise data on employees’ personal devices?
- Are the security warnings issued to employees effective?
- Are we providing enough user education?

Lost or Stolen Devices

The loss of a device used for work, whether it’s a personal or employer-supplied device, can lead to serious security implications, including intellectual property loss that can damage a company’s reputation, undermine its brand, or jeopardize its competitive edge. Breaches of data security compliance measures are another top-of-mind concern for enterprises, as they can reduce customer confidence and lead to costly fines and legal repercussions.

Yet the majority of workers (60 percent) who took part in the *Cisco Connected World—International Mobile Security* survey say that they have recently engaged in risky technology behavior on a device used for work. The most common behaviors include borrowing someone else’s wireless connection when working remotely or from home, allowing a non-employee to use their work device, or leaving their device exposed in a car. And in the past 12 months, roughly half of respondents said that either a company-issued or personal PDA or tablet that they used for work had been lost or stolen. For more than one-third of respondents, either a company-issued or personal smartphone had been lost or stolen.

Overall, respondents believe that losing a company-issued device is slightly more risky than losing a personal device used for work. About two-thirds of respondents said that losing a company-issued or personal device outside the workplace, writing their user access credentials on a piece of paper, or leaving a device exposed in a car were the top risks to corporate security.

Considerations for IT:

- What type of control do we have over devices if they are lost or stolen?

Security Threat Concerns

While the majority of respondents seem to recognize that losing a device outside of work, or engaging in behaviors that could compromise the device or access credentials, could undermine corporate security, survey findings indicate that many aren’t concerned about device-related security—regardless of whether they’re using an employer-provided or a personal device.

Overall, respondents to the *Cisco Connected World—International Mobile Security* survey presented a variety of reasons for not always being concerned about security threats. The top reason: They don't think there is enough risk for concern. And some respondents indicated they weren't always concerned about device-related security because their IT department hadn't informed them of any threats.

Considerations for IT:

- How can we better communicate information about potential device-related security threats?

Attitudes Toward IT at Work

Results for the *Cisco Connected World—International Mobile Security* survey reveal that policies and procedures companies implement to protect against threats vary dramatically. And even when security agreements are in place, they are sometimes ignored, unenforced, or ineffective.

When they were first hired, 58 percent of survey respondents said they were required to sign specific security agreements regarding internal data. While most respondents (77 percent) said they always adhere to those agreements, nearly one-quarter of respondents reported that they did not comply with policies all the time. Among those who did not always adhere to their company's security agreement, the largest proportion (42 percent) indicated it's because they "forget sometimes."

According to the survey findings, most respondents (84 percent) have confidence in their IT department's ability to identify security threats. More than half of respondents said their IT department provided them with periodic training regarding security risks and controls. In addition, roughly half of workers surveyed said their IT department took a proactive role in notifying them about potential risks and threats. As a result, three-quarters of those respondents said they became more cautious.

Considerations for IT:

- How can we enforce policy?
- Is our user training effective—and are we proactive about providing it?

Conclusion

As these research highlights from the *Cisco Connected World—International Mobile Security* survey show, mobility is a complex opportunity that is creating challenges for enterprises and IT departments around the world. There is no straight path to reaching a state of "secure mobility": Every global organization has to develop an approach to mobile security that is part policy, part education, and part technology, and that will support the needs of their workforce and help them to stay productive and achieve key business objectives. And this will likely take time to accomplish.

Meanwhile, many enterprises are making important strides in both evolving their security model to meet the needs of today's connected world and trying to find common ground with employees who are demanding access to applications and devices they want to use for work. As they seek to find "optimal" answers to the many IT challenges and considerations outlined in this paper, they are re-evaluating acceptable use policies and business codes of conduct, putting greater focus on data loss prevention efforts, and working to make enterprise security a top-of-mind concern for all employees, at all levels of the organization.

---

[2] The 2011 and 2013 Cisco Annual Security Reports are available for download at: http://www.cisco.com/en/US/prod/vpndevc/annual_security_report.html.

[3] Cisco 2013 Annual Security Report: http://www.cisco.com/en/US/prod/vpndevc/annual_security_report.html.

Cisco Secure Access

The Secure Access solution from Cisco can help enterprises and their IT departments meet rising user and device demands while minimizing risk and security breaches by building a foundation that connects people anytime, anywhere, using any device. It enables BYOD, cloud, and collaboration to help transform the workspace with confidence.

- A policy-governed unified infrastructure provides consistent secure access policy across an organization's network (wired, wireless, or VPN) for devices and users.
- Efficient security includes additional layers to ensure an uncompromised and highly productive user experience on- or off-premises.
- Simplified management provides extensive visibility to accelerate troubleshooting and allows organizations to focus on innovation with confidence.

The core of the Secure Access solution from Cisco is the powerful combination of the Cisco AnyConnect® Secure Mobility Client, Cisco ASA 5500-X Series Next-Generation Firewalls, the Cisco Identity Services Engine (ISE), and Cisco TrustSec®.

For more information about Cisco Secure Access and its components, go to http://www.cisco.com/en/US/netsol/ns1204/index.html - ~Products.

Cisco BYOD Smart Solution

Cisco is leading the way in helping companies embrace the BYOD phenomenon, offering flexible deployment options for mobility/BYOD solutions and a simple choice of platform or service approach.

Cisco also provides a comprehensive approach to effectively designing, managing, and controlling the access of a BYOD network. The Cisco BYOD Smart Solution provides the most secure, comprehensive endpoint and network lifecycle management system for the enterprise. It simplifies IT operations with end-to-end and network lifecycle management, delivers an uncompromising work-your-way user experience, and enables organizations to secure data with unified policies and the essential controls necessary to support the "beyond BYOD" work environment.

Learn more about the Cisco BYOD Smart Solution.

Cisco's "Any Device" Initiative

Cisco is among the many enterprises around the world working toward secure mobility for all users, no matter where they are located or what device they want to use. Cisco manages more than 64,000 mobile devices today, and employees have the flexibility to choose their device and securely connect to voice, video, and data services from anywhere under an Any Device policy.

Cisco's unfolding BYOD journey has been chronicled in the last two *Cisco Annual Security Reports*.[2] By the time Cisco reaches the final stage of its planned journey, which will take several years, the company will be increasingly location- and service-independent—and enterprise data still will be secure.[3]

METHODOLOGY

The 2012 *Cisco Connected World—International Mobile Security* survey was conducted across 10 countries, in local languages, with more than 4600 participants. Following were the respondents' criteria:

- Resident of Australia, Brazil, China, France, Germany, India, Italy, Japan, the United Kingdom, or the United States
- Aged 21 or over
- Employed full time
- Works for an employer with 10 or more employees
- Not employed in market research, IT consulting, or the nonprofit industry
- Uses company-issued or personal devices for work-related activities
- Works remotely a few times a year

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-728986-01 08/13