

Getting Ready for a Bring-Your-Own-Device Workplace

People get quite attached to their smartphones and tablets. And now state and local government workers have begun bringing their own devices to work to check email, view and edit documents, and more. What are the implications of a bring-your-own-device policy for government?

“At the NASCIO 2011 conference for state CIOs, attendees belonged to one of two camps,” says Jennifer Bremer, who is with Cisco’s state and local government team. “Some were still debating whether to allow employees to use personal devices for work. The others had concluded they couldn’t stop the trend, so they were focusing on how to protect data.”

Device Diversity: Here to Stay

The United States currently has more active cell phones, tablets, and laptops (327.6 million) than people (315 million).¹ It’s not unusual for people to own three or more devices. Fortunately, the proliferation of personal mobile devices can actually benefit government.

“Giving employees a choice of how and when to work increases employee satisfaction, which helps government attract and retain the new generation of workers,” Bremer says. What’s more, a bring-your-own-device policy can reduce costs. Providing productivity applications for employees’ personal tablets, for example, is less costly than buying the devices themselves.

Apply Access Policies to Mitigate Risk

To confidently allow employees to use personal devices for work, state and local governments need to make sure that data is secure both at rest and in motion. Here are some of the questions to ask to prepare for the influx of mobile devices in the workplace:

- **Will you grant different privileges based on the device?** One option is granting full privileges on any device after employees enter one-time passwords. Another is applying different access policies depending on the device type. “The network can recognize whether the device is owned by the employee or the government,” says David Graziano, security solutions manager for Cisco. “To mitigate risk, you might want to allow only Internet access, or possibly email access, on personal devices.” At Cisco, employees can access the network using personal devices, but only if they have registered those devices so that the security team can associate network activity with a person.
- **How will you prevent data loss?** Arguably the best way to mitigate the security risk from lost or stolen devices is to not store any data on the device itself. With the Cisco® Virtual Experience Infrastructure (VXI), employees can use any device to securely access their desktop applications and data, which are physically stored in the data center rather than on the device hard drive.
- **How will you prevent problems from personal devices that are infected?** The Cisco Identity Services Engine (ISE) helps to make sure the device’s antivirus and operating system patches are up to date before granting access to the network. The same solution can block access from devices loaded with bandwidth-hungry applications.



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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. 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. 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. (1005R)

Getting Ready for a Bring-Your-Own-Device Workplace

- **How will you enforce security policy?** Cisco's bring-your-own-device security architecture applies three layers of protection. "It considers the context—user, device, location, and time—to apply policy," says Graziano. "It provides web security by blocking sites with malware and giving you granular control over social networking sites like Facebook and Skype. And it provides a secure, always-on VPN connection."
- **Will you subsidize productivity apps for personal devices?** "Some governments are concluding that application subsidies are a good business decision," Bremer says. "Not only do employees appreciate being able to bring personal devices to work, but governments also save money by purchasing and managing fewer devices."
- **Is the Wi-Fi network up to the task?** If more people are connecting, it's a good idea to revisit the Wi-Fi network to make sure it can handle more simultaneous connections. New wireless solutions from Cisco automatically detect and work around interference caused by microwave ovens, cordless phones, and other devices. An experienced services partner can work with you to assess capacity and recommend upgrades.

To learn more about the Cisco Virtual Experience Infrastructure, visit: www.cisco.com/go/vxi

To read how Cisco IT uses the Cisco AnyConnect™ Secure Mobility Client as part of its any-device policy, visit: www.cisco.com/web/about/ciscoit/work/network_systems/anyconnect_deployment_web.html



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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. 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. 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. (1005R)