Bring Your Own Device: How Do State and Local Governments Address the Proliferation of Employee Devices?

Executive Summary

By the end of 2012, the number of mobile devices will exceed the number of people on the planet.[1] And in increasing numbers, government employees are using their tablets and smartphones for work–whether or not their employer has a formal bring-your-own-device (BYOD) policy.

Is BYOD a bane or boon for government? In July 2012, Forrester Consulting, in a poll sponsored by Cisco, surveyed 498 government employees around the world to understand their experiences with BYOD. Survey participants worked in the United States, Canada, Mexico, Brazil, United Kingdom, Germany, United Arab Emirates, Saudi, South Africa, India, Australia, South Korea, China, and Japan.

This report, intended for state and local government IT leaders around the world, presents the results of the survey and how they pertain to government goals for citizen service, workforce productivity, public safety, recruiting top talent, and cost containment.

- Mobile devices are everywhere, including government
- Failing to implement a BYOD policy is risky
- When properly managed, BYOD can cut government costs
- Allowing employees to use their own devices helps to increase efficiency and citizen satisfaction
- An employment “perk” that especially appeals to millennials–and costs nothing!
- BYOD success factors

Mobile Devices Are Everywhere, Including Government

Soon there will be more mobile devices than people.[2] Mobile data traffic more than doubled in 2011 and is expected to double again in 2012.

The mobile explosion has touched both the public and private sectors. A Forrester Consulting survey of government employees around the world revealed that 94 percent of respondents regularly worked on laptops, 63 percent used smartphones, and 18 percent owned tablets, a rapidly growing portion.

The new generation of workers, so-called millennials, are especially avid users of mobile devices. In a 2011 survey of 3000 college students and new graduates around the world, conducted by Cisco, 64 percent would choose an Internet connection over a car if forced to make a choice.[3] And 66 percent of the students and 58 percent of the new employees identified a mobile device, such as a smartphone or tablet, as the most important technology in their lives.

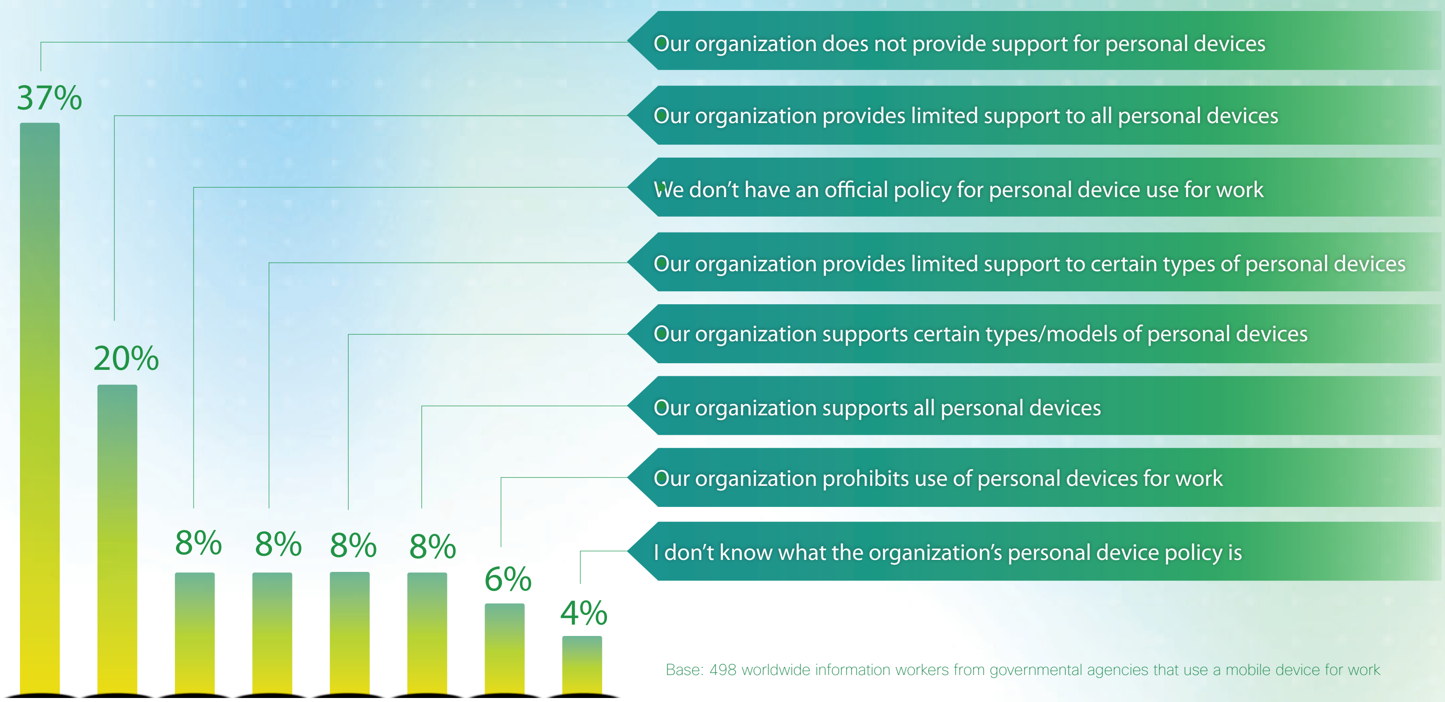
Mobile devices and new mobility applications support a wide range of government priorities:

- **Continuity of government:** If employees cannot work in the office because of weather conditions, pandemic, or disasters, they can work from anywhere by using a personal device to access a "virtual desktop" that resides in the government data center.
- **Citizen service:** Employees with mobile devices can respond to citizen requests from anywhere instead of waiting until they return to the office, improving responsiveness and citizen satisfaction with government.
- **Public safety:** First responders can use tablets with video and collaboration applications to increase situational awareness.
- **Workforce productivity:** New employees become productive more quickly when they can use a familiar device.
- **Cost savings:** Many employees are willing to assume some or all the hardware and monthly service costs in exchange for the freedom to "work your way." (Read more.)

Ignoring BYOD Is Risky for Governments

Despite the explosion of mobile devices, more than half of the respondents in the Forrester survey (57 percent) said their governments provided limited or no support. Six percent said their employers prohibit mobile devices outright. And about one in five acknowledged that their organizations have no official BYOD policy (Figure 1).

Figure 1 What Is Your Organization's Policy for Enabling the Use of Employee-Owned Devices for Work Purposes?



Base: 498 worldwide information workers from governmental agencies that use a mobile device for work

Prohibiting personal devices is risky, as is not publishing a clear policy. That's because when employers prohibit personal devices, employees find workarounds. In the Forrester survey, 3 out of 10 government workers in this situation admitted that they find "alternative ways" of using their device for work.

The risks of not implementing a security policy include exposure of sensitive citizen or government information if:

- The device is lost or stolen
- Transmissions are intercepted because the wireless network is not secured
- The device is infected with malware, an emerging problem for mobile devices

In a BYOD world, governments need policies to protect network access and information.

Properly Managed BYOD Programs Can Cut Government Costs

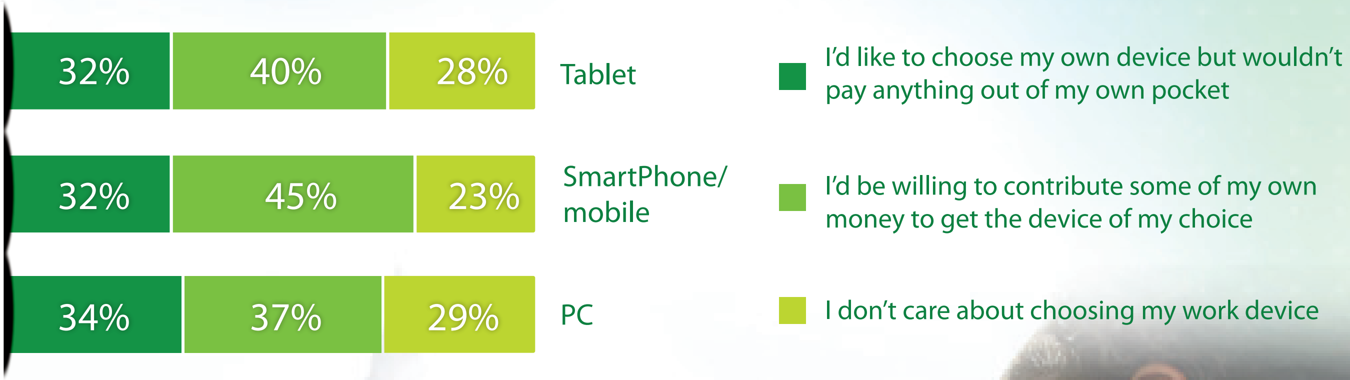
If properly managed, BYOD programs can lower capital and operational costs by replacing certain government-owned devices with personal devices. According to Gordon Bruce, CIO of the city and county of Honolulu, "[When workers bring their own devices for work], we won't have to pay for them, which means the taxpayer won't have to pay for them."[4]

In the Forrester survey of government workers, 59 percent who use smartphones at work and 47 percent who use tablets paid for the devices themselves. Another 6 percent of smartphone users and 12 percent of tablet users shared the costs with their employer. And even more are willing: Roughly 70 percent of survey respondents said they would pay for some or all their smartphone, tablet, or laptop to have a choice. Figure 2 summarizes some of this data.

Employees are also agreeable to paying some or all monthly service provider costs: 47 percent pay fees themselves, while 9 percent share it with their organizations.

After encouraging BYOD for just one department, the state of Delaware reduced the expenses associated with smartphones by 45 percent, and reduced overall department wireless costs by 15 percent.[5]

Figure 2 The Majority of Government Employees Want to Choose Their Device and Many Will Help Pay



Base: 494 worldwide information workers from governmental agencies that use a mobile device for work

Allowing Employees to Use Their Own Devices Helps to Increase Government Efficiency and Citizen Satisfaction

Employers in the public and private sectors regard productivity gains as a major motivator for BYOD programs.[6] In the Forrester survey of government workers:

- 60 percent agreed that BYOD would help them be more flexible.
- 57 percent said that being able to work on a personal device boosted productivity—for example, by enabling them to respond to email from home before or after work.
- 55 percent believed that getting to work on their own devices makes them more resourceful.

New enterprise collaboration applications for iOS and Android devices help to make business workflows more efficient. For example, employees who need a quick answer to resolve a citizen issue can use Cisco® Jabber™ to see if coworkers are available and then just click to send an instant message, avoiding the delays of email and voicemail. Distributed project teams can meet with an in-person experience by using their tablets to join Cisco TelePresence sessions with high-definition video. And employees can work securely from anywhere when they use a tablet to work with a virtual desktop housed on Cisco® Virtual Experience Infrastructure (Cisco VXI®) in the government data center.

An Employee Perk That Costs Nothing!

In addition to boosting productivity, government BYOD programs can help governments recruit talented new college graduates and boost workplace morale—without increasing costs. It's an urgent issue, because fewer millennials are pursuing careers in government, gravitating instead to the private sector, graduate school, or nonprofit work.[7]

In the Forrester survey, more than half of government workers (52 percent) said that using their own devices for work increased job satisfaction. And 44 percent indicated they would be more likely to work for an employer that allowed them to bring their own device to work.

BYOD Success Factors

While BYOD policies vary by government, most successful BYOD programs include the elements described in Table 1.

Table 1 BYOD Success Factors

Success Factor	Enabler	Cisco Solutions
Consistently good user experience	Device acceleration Optimized wireless performance Secure VPN access	Cisco Wide Area Acceleration Services (WAAS) Mobile Cisco CleanAir™ Technology Cisco AnyConnect® Secure Mobility Client
Security	Policy enforcement based on user's role, type of device, time of day, and more Protecting data in motion Web security Email security	Cisco Identity Services Engine (ISE) Cisco Adaptive Security Appliance (ASA) CX Context-Aware Firewall Cisco Aironet® Wireless Access Points Cisco Cloud Web Security Cisco Cloud Email Security
Collaboration capabilities	Unified interface for voice, video, and IM Consistent, simple user experience	Cisco Jabber™ and Cisco Jabber Video for TelePresence® Cisco Jabber is available for Windows, Mac, iOS, and Android operating systems
Ease of management	Managing wireless, wired, and VPN networks from one interface Flexible policy enforcement	Cisco Prime™ Infrastructure Cisco Identity Services Engine (ISE)
Alignment of BYOD program to government business objectives	Architecture strategy, assessment, and design	Cisco Unified Workspace Services for State and Local Governments

To learn more about the Cisco BYOD Smart Solution for government, visit:

www.cisco.com/go/govbyod

[1] Cisco Visual Networking Index (VNI)

[2] Cisco Visual Networking Index (VNI)

[3] Cisco Connected World Technology Report

[4] http://www.digitalcommunities.com/magazine/A-Look-at-Personal-Mobile-Devices-in-the-Office.html

[5] http://www.whitehouse.gov/digitalgov/bring-your-own-device#delaware

[6] http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_forrester_measure-value-of-consumerization.pdf

[7] *Minding the Leadership Gap: Attracting Millennials to the Federal Government,* Government Business Council, March 2012

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.**