

A Forrester Consulting Thought Leadership Paper Commissioned By Cisco

BYOD in Government: Prepare For The Rising Tide

September 2012

FORRESTER

Headquarters | Forrester Research, Inc.
60 Acorn Park Drive, Cambridge, MA 02140 USA
Tel: +1 617.613.6000 | www.forrester.com

Forrester Consulting
Making Leaders Successful Every Day

Table Of Contents

Executive Summary.....	2
Government Employees Use Personal Devices for Work Purposes	2
Employee Benefits Drive Use of Personal Device; Cost Savings Are Less Clear	5
Despite Benefits, BYOD Strategies and Governance Policies Remain Scarce	7
If It's Really Inevitable, How Do You Get There?.....	10
What it means: Use BYOD to Prepare for the Workplace of the Future.	11
Appendix A: Methodology.....	12
Appendix B: Endnotes.....	12

© 2012, Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. For additional information, go to www.forrester.com. [OrderID]

About Forrester Consulting

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit www.forrester.com/consulting.

Executive Summary

Forrester's study of the use of personal devices for work purposes within government organizations has yielded the following key findings:

- **Government employees use personal devices for work purposes.** According to the recent Forrester survey, 58% of information workers in government use a smart phone for work purposes that they have purchased without considering what the organization supports. Government IT decision-makers must face the reality that employees are bringing their own devices (BYOD) to work.
- **Yet BYOD policies are nascent if not non-existent.** Few organizations have their head in the sand about the reality of BYOD. But most are still in research and pilot mode with limited trials of device subsidies, policy-based application access and mobile device management. Few, if any, government organizations have agency-wide BYOD programs, and according to the recent survey only 6% of smart phone users and 4% of mobile phone users using personal devices received a subsidy.
- **Security concerns impede policy roll-out for many organizations.** The biggest worry among government IT decision-makers is security of applications, and the data within them: how do we secure the device? The applications? And the data? How do we ensure that information isn't transferred to unsecure locations?
- **BYOD implications extend beyond IT to human resources and legal concerns.** But the concerns of IT leaders didn't stop with technology. Liability is a major concern: who is liable in case of theft or loss of a device? HR implications are another concern: Use of personal devices blurs the dividing line between work and life, and violates strict working conditions imposed in some countries by public sector unions.
- **CIOs craft BYOD strategies to enable productivity while protecting application and data security.** Government IT decision-makers recognize the inevitability of BYOD and set out to define their terms. But the BYOD trend has raised additional questions around the workforce and the workplace of the future—a broader spectrum of issues that government organizations will have to address.

Government Employees Use Personal Devices for Work Purposes

The use of personal devices for work purposes is almost universally considered inevitable across all industries¹ and that includes government employees. Although government organizations have not typically been known as hotbeds of technology, their retro status is changing as employees bring their own devices to work. Some early adopter public sector organizations already provide device choice through a device and services catalogue from which employees select the device they need, and are authorized to purchase. But even those organizations who embrace flexibility and choice are being pushed by demands for the use of personal devices. For example, if smartphones or tablets are not in the catalogue, employees request to use their own.

"BYOD is an inevitable outcome. The challenge is how you manage the transition." (CIO at a UK local county council)

A survey of government employees indicates that this trend is prevalent across government organizations.

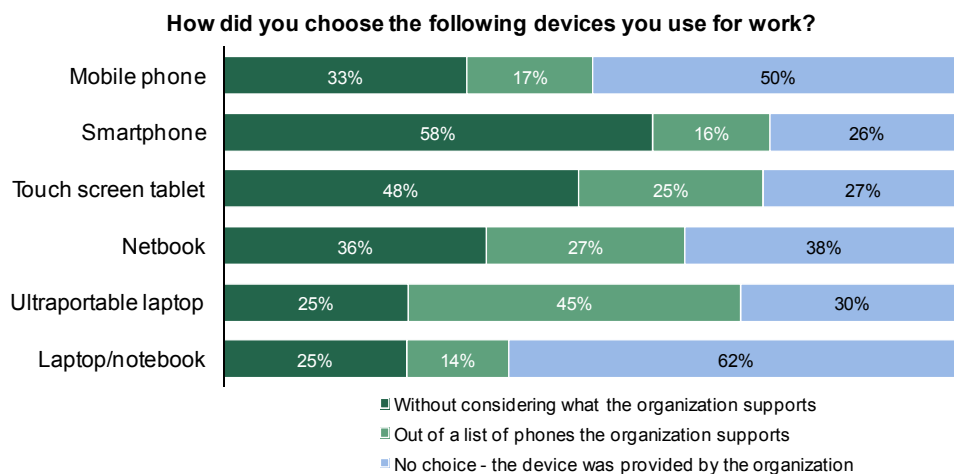
- **While government organizations issue mobile phones and laptops to employees...** 62% of government information workers are issued laptops with no choice of make or model. For mobile phones 50% are issued a standard device (see Figure 1). In the case of standard issue devices, government organizations typically pay for them (see Figure 2).
- **...most government employees use smartphones and tablets they've purchased themselves.** According to the survey, 58% of information workers in government use a smart phone that they have purchased without considering what the organization supports. For tablets, 48% purchase their own without consideration of support. And, they pay for the devices themselves: 59% of smart phone and 47% of tablet users report that they paid for their own devices. Employees are often filling the gap with devices they purchase themselves. As a desktop services director at a provincial government department in Canada noted, *"We see more demand for tablets because we don't offer them right now."*
- **Device choice through a services catalogue and shared device costs are less common.** Some government organizations do provide choice of devices: 25% of tablet users and 16% of smart phone users purchased their devices from a list of shared devices. Purchases from these services catalogues are most common for ultraportable laptops.
- **Elected leaders, senior management and mobile workers drive demand...** Generally, demand to use personal devices comes from those who need to be mobile and contactable: managers in meetings, case workers out in the field, tech support after hours and weekend. But overwhelmingly we heard that senior management and elected officials push to use their personal devices as well. And, the pressure from management and elected officials often carries more weight.
- **...Primarily to check email and calendar appointments....** Government executives and information workers want to keep up on email and urgent communications when travelling or out of the office. But increasingly, employees used to reading personal email on a smart phone also want access to their work email on their personal device in order to "check in" on their own time.

"Email and a few business applications top the list of use-cases. Executives are looking to catch up on email and urgent communications when travelling. They are also using these devices to read and update documents such as proposals and presentations." (Deputy Director at a UK central government organization)

- **... with some demand for access to line of business apps and data.** Demand for access to applications and data vary widely across organizations. Local governments see the need for more flexible access to CRM or case management software, where social services employees find it useful to manage cases from personal devices while on site. Some research organizations work in collaboration with external international organizations whose researchers need access to internal data on their personal devices.
- **Mobile access on either cellular or wi-fi networks dominates.** Most IT decision-makers surveyed anticipate a greater use of personal devices through mobile access. A select few employees, such as heavy graphics users or application developers, may request the use of a specific device in their office. But the vast majority of government employees using personal devices for work do so via mobile access.

Figure 1

The Majority Of Government Employees Independently Choose The Smartphones They Use For Work Purposes

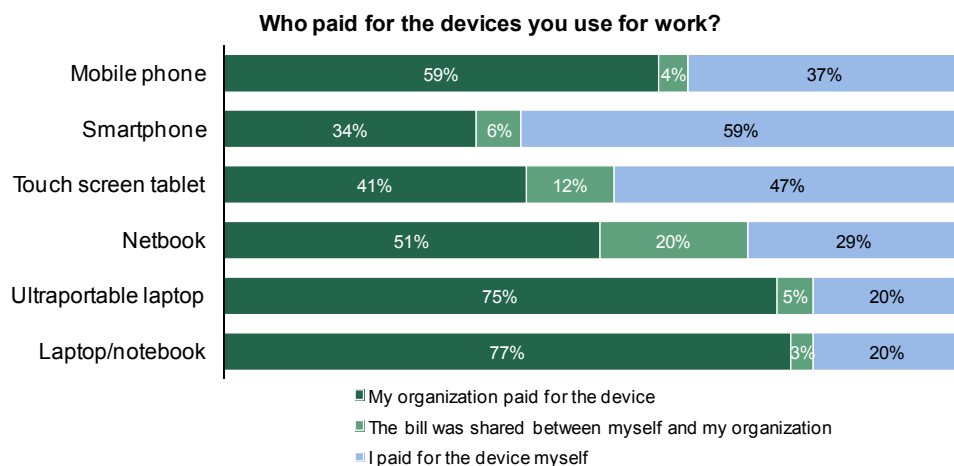


Base: 498 worldwide information workers from governmental agencies that use a mobile device for work

Source: A commissioned study conducted by Forrester Consulting on behalf of Cisco, June 2012

Figure 2

It's all or nothing: Few government employees receive subsidies for device purchases.



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

Source: A commissioned study conducted by Forrester Consulting on behalf of Cisco, June 2012

Employee Benefits Drive Use of Personal Device; Cost Savings Are Less Clear

Employees – and the benefits they expect – drive the use of personal devices in government organizations.

- **Personal devices are mainly being used today for convenience...** For many employees, consolidating work and personal use into a single device eliminates the need to juggle multiple devices and this convenience extends to most government employees. According to an IT decision-maker at a local government council in the UK, even those who weren't originally perceived to be mobile workers and didn't have a council-issued device began to use their personal devices because *"if I could, wouldn't that be better"*. A similar observation was made by the head of IT in a municipal agency in Canada, *"Even when someone may not need a tablet or smartphone to do their day-to-day work, having one may help manage life better. Moreover, new employees who have used a smart phone or tablet elsewhere – either in a former job, at school or at home – expect to maintain the convenience to which they've become accustomed"*.

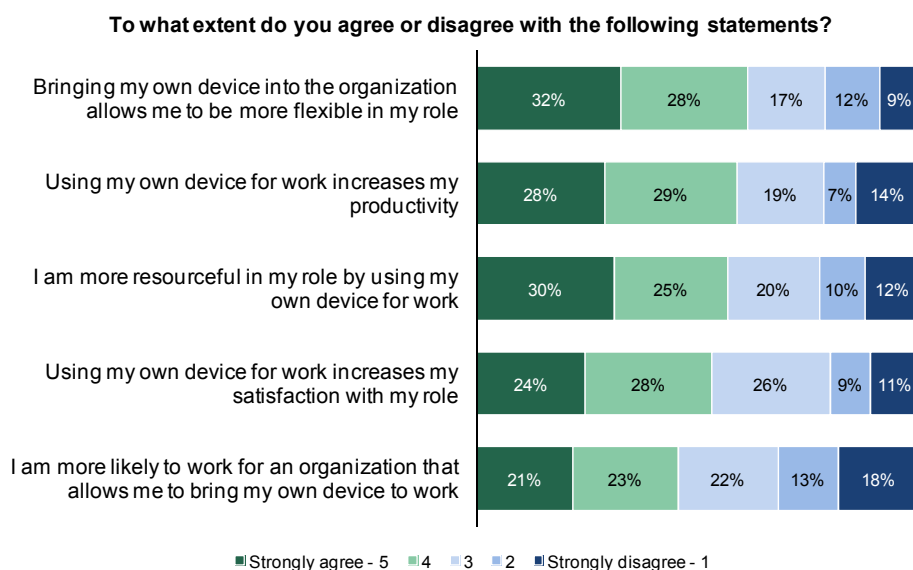
Another local government CIO noted, *"The business case [for BYOD] usually tries to formulate around reducing paper but in reality it's a convenience thing"*.

- **... and with the expectation of increased flexibility, productivity and resourcefulness.** According to the current study, 60% of respondents reported that bringing their own device into the organization allows them to be more productive in their role; 57% believe that using their own device makes them more productive; and, 55% believe that they are more resourceful if able to use their own device (see Figure 3).
- **Personal device use increases job satisfaction but doesn't always influence job choice -- yet.** Of government information workers who use mobile devices for work, 52% report increased job satisfaction as a result. That figure is expected to grow, as is the 44% who report that the ability to use a personal device will positively influence job choice. As the director of IT for a national health organization noted, *"The worker demographic change in coming years will mean that potential employees will be swayed by technology, and how forward thinking a future employer is in terms of what is allowed and not allowed. Perception on flexibility and forward thinking will be critical to finding talented staff"*.

And, as the head of IT for a UK county council speculated, *"Try to resist and you will see what it does to satisfaction!"*

Figure 3

Employees See BYOD As Increasing Flexibility, Productivity And Resourcefulness



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

Source: A commissioned study conducted by Forrester Consulting on behalf of Cisco, June 2012

- **Most government CIOs don't have a clear picture of the ROI or cost advantages of BYOD.** Cost benefits depend on the device acquisition policies. In a US state government, uptake of a new policy to allow use of personal devices led to an 18-20% reduction in government-issued devices. That's cost savings. But several CIOs surveyed believe that the key cost saving potential lies in day by day support: *"We don't have to provide the same level of support on BYOD. People are now responsible for their own devices"* (Director Corporate IT at a national health organisation). The perception that support costs will be lower, however, is not tested.

And, in any case, as the IT director of a US state observed, *"It would be an exercise in justifying to our policy makers that there is a cost benefit of driving state owned equipment down by allowing employees to use personal devices and the management of those devices. Cost-benefit analysis is more straightforward in the enterprise; it just doesn't work the same way in state government."*

- **But a comprehensive IT strategy including BYOD and improved security can reduce costs.** UK Cabinet office... Consumer approach would dramatically reduce the cost. We calculated that running consumer kit and providing a shared desktop for LOB apps is 80% cheaper than running standard locked down devices. And experience is 100x better. 81% IT cost saving we saw. Per individual we're saving about 1200 pounds a year cause comparatives are expensive (restricted device costs were 1600 a year for a locked down laptop and support services on the OS)

Despite Benefits, BYOD Strategies and Governance Policies Remain Scarce

While few organizations prohibit the use of personal devices outright, the majority provide limited or no support. Only 6% of government employees surveyed report that their organization prohibits the use of personal devices (see Figure 4). Yet 37% report that their organization provides no support; 36% provide some support – either support for some devices or limited support of all devices. And, only 8% report that all personal devices are supported. And, although only 8% of government employees report that their organization does not have an official policy for work-related use of a personal device, those policies are not yet well defined and in most cases are still works in progress.

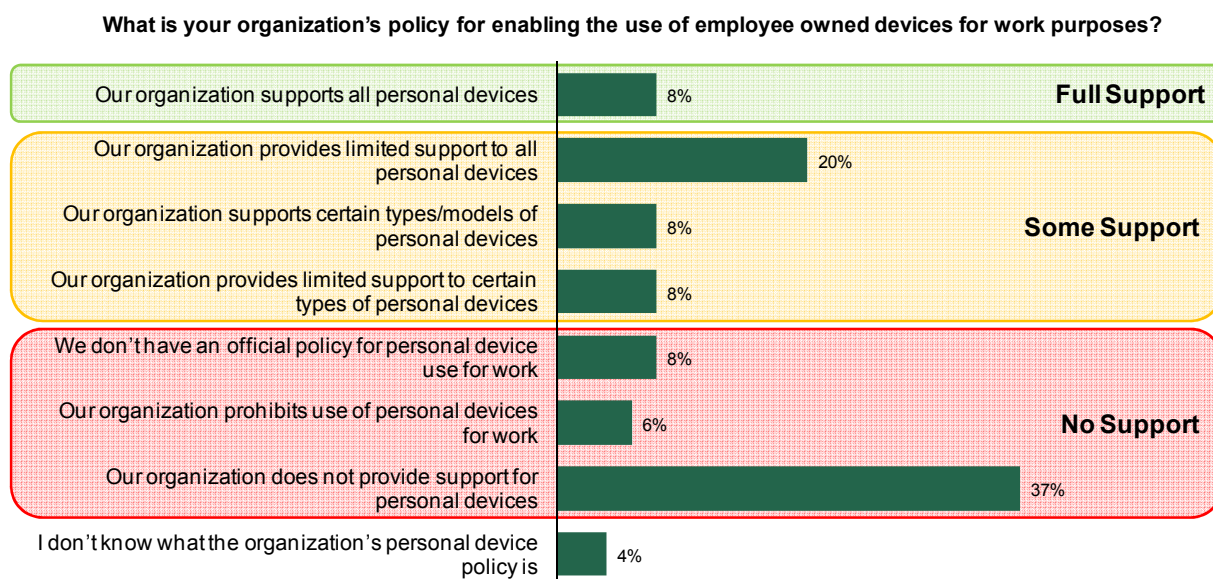
“We are headed in the direction of BYOD but we are taking a very cautious approach.” (IT policy advisor, Canadian provincial government)

CIO and IT management in government organizations report that:

- **Government organizations remain in research and planning mode with regard to BYOD.** Of the 11 government organizations interviewed for the current study, not one in North America had a formal policy governing the use of personal devices. Several had appointed staff members to develop strategy and formulate a policy. But most were in the early days of research and planning. Organizations in the UK were much farther along. One exception was a UK county council. While they did not call their policy BYOD, they have a comprehensive “mobile and flex” policy including thin client architecture, two factor authentication for applications, and guidelines for personal responsibility. Another national UK organization which openly allows informal use of personal devices plans to roll-out its formal policy within 6 months.
- **Draft policies vary widely across government organizations – with device subsidy a sticky issue.** Some organizations are well down the path of drafting policies with pilot programs targeting specific provisions: one US federal organization is conducting 35 separate pilots to evaluate program alternatives. At the other extreme, one provincial government in Canada reported that they would start to explore more hands on in the next year. One policy element that is difficult to nail down is the device subsidy: how much? And how often? But others still don’t even bother. A university in the southern US indicated that they were writing it into job descriptions that applicants were required to provide their own device, typically a smart phone, for the job.
- **But delays in central BYOD strategies and guidelines can lead to policy proliferation.** One concern among some organizations was a proliferation of incompatible policies. Several central IT departments included in the current study feared that smaller, more nimble agencies within their larger organization were ahead of the curve. *“They can be off and running in a short period of time and don’t think about a larger policy, whereas the central IT department is looking at it more holistically, and more slowly.”* In these cases, consolidating and rationalizing the competing policies could be tough.

Figure 4

Few Organizations Prohibit Use Of Personal Devices; But Majority Provide Limited Or No Support



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

Source: A commissioned study conducted by Forrester Consulting on behalf of Cisco, June 2012

Security Concerns Top Impediments to Formal Policy Roll-Out

For most IT decision-makers, the biggest impediment to the use of personal devices in government organizations is the security implication. Government data security and citizen privacy issues are top concerns.

"Security is the reason we don't currently have a policy... ensuring the security of state information and applications and protecting the information of individuals. Privacy and security concerns have slowed the process." (CIO US state government)

- **BYOD would bring a proliferation of devices types and operating systems....** Currently organizations are able to control their IT environment. Many lock down device and operating system options. Organizations fear they don't have the expertise to secure a more diverse environment. And, IT views personal devices as "non-trusted."
- **... and greater temptation for employees to bypass security rules.** It seems that the lack of trust doesn't end with the device. Many organizations are concerned with employees "browsing up," e.g. looking at more sensitive information than permitted. The reaction is to limit any form of bring-your-own to people who do not access any protected or restricted information. Other organizations worry about increased use of "the cloud." They envision employees uploading information or saving documents onto public clouds for access via a personal device, and the popularity of consumer cloud storage suggest that this concern is not unfounded. The

use of public clouds also brings concerns about jurisdiction and cross-country data flow, especially data stored in US territory.

- **CIOs investigate device management with emphasis on sandboxing government applications and data.** As personal devices are increasingly used for government work and government-issued devices for personal use, IT decision-makers worry about the blurring of information ownership and liability.² IT organizations explore mechanisms to partition or sandbox the data and applications associated with each use. Many organizations are currently investigating and in some cases piloting the currently available solutions.
- **Others explore new security architectures with protection at the application and data level.** The CIO of a US federal agency envisions secure applications sitting alongside applications that are wide open, without having to protect the device. The security architecture implements controls on an application by application basis. “Long term we don’t want to protect end points nor will we have firewalls. The security will be built into the data and applications. We should be able to do the vast majority of work by changing the security architecture.”
- **Network security and capacity remain an open question.** Most IT decision-makers interviews were less concerned about network security or capacity. Some focus on security at the application and data layer in order to establish more granular controls. Others provide access to the internal wireless network for a personal device through the “guest wireless access.” “Guests” are able to do email and calendaring and look up things on the internet but they cannot change data or configurations. Most are still making decisions about wireless and networking, recognizing that capacity increases will be necessary to accommodate increased traffic.
- **Although not top of mind, device diversity will exacerbate application integration challenges.** Few CIOs interviewed have spent much time thinking about how BYOT affects application integration and development. However, the use of personal devices will dramatically increase the number of integration scenarios. For example, enabling business applications for mobile devices used to be focused on standardized corporate devices. Now, the varieties of employee-owned devices require multiple mobile integration implementations.³

And Implications Extend Beyond IT: Political, Legal And HR Concerns Often Dominate.

The use of personal devices by government workers raises issues that extend beyond technology. IT decision-makers are concerned about the political, legal and HR implications of a formal policy.

“Our concerns aren’t about the technology; it is the HR and legal requirements and implications. If a mobile device is compromised, we worry about how well we have partitioned the device and what government controls we have put on it. Who is responsible for compromised devices?” (CTO at a US federal government research agency)

According to those interviewed, the use of personal devices and formal policies governing their use:

- **Challenge the classic model of a 9-5 government worker; some public sector unions object.** As several CIOs mentioned, government organizations are often staffed by public sector union members. In their collective bargaining agreements, there are rules as to how many hours a day employees can work. Unions are not

supportive of BYOD programs because they feel that it is a way for the organization to make employees work more.

- **Raise concerns among government leadership about public perception.** Government organizations already face the scrutiny oversight committees and of their constituents over the use of technology, and their leaders worry about public perceptions of BYOD. As one CIO noted, “There was a lot of attention by our legislature in the past for cell phone use. Should civil servants be running around with the latest and greatest in technology, especially during times of austerity?”
- **Complicate government compensation and expense reimbursement policies.** In addition to the questions of how much and how often, several CIOs mentioned concerns about implication of device subsidies or reimbursements on compensation. If employees received a stipend every few years, would these be considered income and taxed accordingly? And, what happens if an employee leaves after receiving the stipend, or before the end of a smart phone contract. Do they pay it back? Who’s responsible for the remaining contract or cancellation fees? For many agencies, these remain open questions.
- **Distort the division of personal and work-related information, and responsibility.** If a mobile device is compromised, the sandboxing or partitioning come into play. What if personal information is lost or compromised? Who is ultimately responsible for the device? And, for replacement? These questions continue to plague government leaders.

If It’s Really Inevitable, How Do You Get There?

The use of personal devices for work-purposes is increasing, even in government organizations. It is widely accepted that over time new employees will request the use of the device they know. However, the collective research by IT decision-makers in government provides a valuable starting point for embarking on the journey toward BYOD.

“We know BYOD is coming and we are setting the stage ... As new people come into the government – the new generation – they are used to a new way of working We try to position ourselves as an organization that is an attractive employer”. (IT policy advisor, Canadian provincial government)

Here are some observations on how best to set the stage:

- **The process is evolutionary not revolutionary.** There will not be a big bang, neither in tightly controlled nor in more open IT environments. Organizations can neither force every employee to BYOD; nor can they resist the trend completely. The process will evolve over time, perhaps work group by work group. Expect to see a trend similar processes in the shift to personal computers, and from desktops to laptops.
- **Policy must not wait; guidelines must be incremental and compatible, and the process collaborative.** As central IT organizations research options and craft comprehensive strategies and policies, lower-level agencies begin to do their own thing. Smaller agencies can react much faster, and end up ahead of the curve. A proliferation of policies then makes consolidation and rationalization across agencies difficult. If this is the case, it may take a legislative or gubernatorial act to make that happen. Best to avoid the scenario.

- **Ultimately, however, policy guidelines must be comprehensive but can evolve over time.** The most prepared organizations are those which have already embraced flexible work environments with mobile devices and thin client architectures accessible from government or home offices. Security mechanisms to support remote access set the stage for the use of personal devices. Device management software which forces sandboxing or segmentation for business and personal use provide the next step. And, a granular application and data security policy ensure appropriate access to government information.
- **Couple BYOD with a community-based support model.** Most government organizations are looking to keep management of BYOD programs in-house in the first instance. That said, many organizations are concerned about their own limited resources and lack of capabilities and expertise. IT departments fear the thought of supporting the universe of possible devices. However, several have embraced the “friend down the corridor” approach which encourages end users to help each other – a community support model. Renegade users of unsupported operating systems have traditionally resorted to this approach. Online forums and colleagues can offload support and training needs.
- **Leverage existing resources to inform strategy and policy.** The recently launched Federal Government Bring Your Own Device Toolkit is a product of the Digital Services Advisory Group and Federal Chief Information Officers Council designed to support federal agencies implementing bring your own device programs. The Toolkit provides guidelines for developing policy and case studies of early adopter agencies.⁴ The National Association of State CIOs teamed with a mobility solution provider to develop a BYOD Best Practices Guide to assist state governments in their BYOD strategy and policy development.

WHAT IT MEANS: USE BYOD TO PREPARE FOR THE WORKPLACE OF THE FUTURE.

While the initial push is toward greater mobility, government IT leaders can use demand for personal devices as a catalyst to review the broader work environment. A flexible work environment doesn't stop with choice of device but includes modes of collaboration and the tools to support the way that employees prefer to work with each other, with partners and suppliers and with constituents. And, that environment isn't limited to technology. Preparing for the workplace of the future requires broader thinking about how best to organize work spaces and even real estate assets. The workplace is changing, and employees demands for the ability to use their personal devices is merely the first step.

Appendix A: Methodology

In this study, Forrester conducted an online survey of 498 government workers across the US, Canada, Mexico, Brazil, the UK, Germany, UAE, Saudi Arabia, South Africa, India, Australia, South Korea, China and Japan to evaluate the demand for Bring-Your-Own-Device (BYOD) initiatives in public sector workers. Questions provided to the survey participants asked about how they choose their devices for work, if their organization enables the use of their personal devices for work and what benefits they have realized from using personal devices for work.

The online survey was followed by interviews with 11 public sector CIOs asking them about the current state of BYOD in their organizations, the pain points associated with enabling BYOD and the benefits realized to date from investments. The study was completed in September 2012.

Appendix B: Endnotes

¹ According to Forrester's Forrsights Workforce Employee Survey, Q4 2011, 43% of employees bring their own devices for work purposes, increasing. See the June 12, 201 Forrester report "Charting The Rising Tide Of Bring-Your-Own Technology" ,

² Right now, the ownership of corporate information on an employee's personal device is murky from a legal perspective. Suppose an employee has a personal device that he paid for but it links to corporate email. Then imagine that the employee loses it, so the company wipes the device, and in the process deletes valuable personal information. Ultimately, this type of unilateral action by IT will be the basis for a landmark court case to determine data ownership and liability. See the June 2012 Forrester report "Charting The Rising Tide Of Bring-Your-Own Technology."

³ See the June 2012 Forrester Report, ".Charting the Rising Tide..."

⁴ See <http://www.whitehouse.gov/digitalgov/bring-your-own-device>.