

HOW GOVERNMENTS CAN TURN BYOD FROM A CHALLENGE INTO AN OPPORTUNITY

Joseph Petroski
Senior Director of Sales Engineering
CellTrust Corporation

Bring your own device (BYOD) is not new to government organizations. For years, employees have used their own computers and laptops for work. What has changed is the dramatic rise in mobile device use for both personal and professional interactions. As a result, state and federal government agencies are looking at new ways to support BYOD deployments.

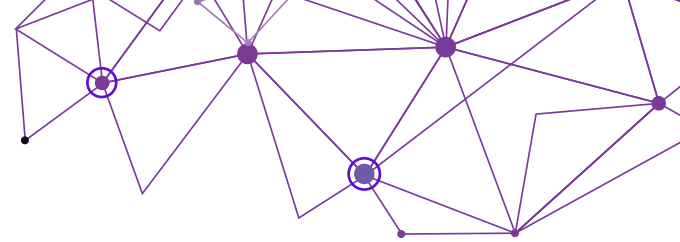
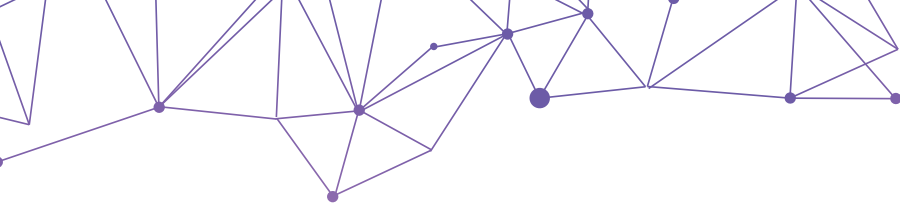
For many government employees, consolidating work and personal use into a single device creates an advantage by eliminating the complexity, security risks, and inconvenience of managing multiple devices. According to a Forrester Research survey on BYOD in Government, 60 percent of government employees reported that bringing their own device into the organization allowed them to be more productive in their role. Additionally, 55 percent believe that they are more resourceful if they are able to use their own devices.¹

Ultimately it's a win-win: government agencies, under the watchful eyes of constituents, can reduce spend on mobile devices, while on-the-go employees get to use their device of choice to help increase connectivity and productivity.



“While I’m not advocating working 24 by 7, it is just more comfortable to sit and do timecard approvals on a Friday night in the comfort of your home instead of during the prime time work day when your attention should be on more complex and business-oriented issues,” U.S. Equal Employment Opportunity Commission CIO Kimberly Hancher said in July 2012.

Since the introduction of BYOD two things have happened. First, government agencies have helped refine the BYOD strategy by grappling with a variety of challenges, particularly security and transparency. The ways they’ve overcome those challenges are worth studying – not only by other government agencies that are considering implementing a BYOD policy, but also by enterprises.



Second, the BYOD category has expanded beyond smartphones and tablets and into wearables, such as smart watches and glasses. These new types of devices have additional considerations and challenges, including supporting new and niche operating systems such as Tizen.

Most government agencies currently support their BYOD deployments with an enterprise mobility management (EMM) platform, a category that includes mobile device management (MDM) and mobile application management (MAM) products. These tools are useful for remotely wiping agency data if a device is lost or stolen and pushing out patches instead of relying on employees to download them. They're also must-haves for enforcing security policies such as FIPS and Common Criteria.

EMM platforms were around long before the BYOD trend began, and arguably BlackBerry was the most widely used. Most agencies used BlackBerry smartphones primarily or exclusively, so using the same vendor's EMM platform was a natural choice.

Today, however, agencies need EMM platforms that can support a wide variety of operating systems (OS) and device types, not just BlackBerry. This need even extends to agencies that still prefer BlackBerry because there are now versions of that OS that can run Android apps.

The expansion in OS variety includes a fundamental change in how security is addressed. With a single OS, a hardware-centric security approach made sense. With multiple OSes, software is a better approach because it provides more flexibility and capability.

This doesn't necessarily mean that government agencies need to rip out their legacy, single-OS EMM. Those platforms might be worth keeping if an agency expects to still have a high percentage of devices running on the legacy OS—even after implementing a BYOD policy. In that case, it's important to look for a multi-OS EMM solution that's interoperable with the legacy platform. That compatibility helps ensure that policies can be applied consistently across all devices, and minimizes the need for manual intervention by IT staff to make the new coexist with the old.



With a single OS, a hardware-centric security approach made sense. With multiple OSes, software is a better approach because it provides more flexibility and capability.

LOOKING BEYOND EMAIL AND BROWSING

When selecting an EMM platform for BYOD, agencies should look beyond the OS and device types it supports. It's equally important to also make sure that the platform supports the widest possible variety of communications types. For example, many EMM solutions secure only email and browsing, leaving voice calls and text messaging vulnerable to data breach, whether intentional (hacking incident) or accidental (lost device) data breaches. Those shortcomings can cause agencies to run afoul of compliance with Open Records laws, which require government organizations to capture and archive mobile communications, including those of officials, which are a matter of public record.

Government organizations also shouldn't overlook how BYOD affects archiving. Many municipalities don't realize that text messages between council members during a public meeting must be saved. An EMM solution that can't archive text messages puts those cities at risk of violating the Freedom of Information Act and other transparency laws.

At a minimum, government agencies should focus on solutions that can encrypt and archive mobile messages and calls, regardless of whether they go over cellular networks or Wi-Fi. EMM solutions that make the cut should be scrutinized for how they enable compliance-required encryption and archiving. But that's not always so clear cut. Government needs to assure employees that only agency data is being preserved, ensuring that employees' personal mobile lives stay personal.



Personas are an ideal way to ensure security and support compliance while respecting employee privacy.

For example, the ideal solution will balance compliance with employee concerns about having their personal calls, messages, browsing, and emails swept into the same archive as their work communications. These concerns shouldn't be underestimated because experience shows that they'll cause employees to look for ways to circumvent policies to protect their mobile privacy. When they do, it's not uncommon for work communications to get dragged out of the EMM solution's reach. And this can lead to a lose-lose scenario: agencies at risk of not meeting compliance and employees violating policies. The solution? Personas.


Personas are an ideal way to ensure security and support compliance while respecting employee privacy. Two personas can be created on each device: one for all work-related apps and communications, and another for all personal apps and communications. This separation enables government IT departments to apply policies only to the work persona on an employee-owned device, such as archiving only councilmember-to-councilmember text messages. This architecture also enables organizations to secure communications such as work-related text messages and emails so they can be viewed only by authorized parties.

THE ISSUE OF PHONE NUMBERS

When government organizations are developing BYOD strategies and policies, they frequently overlook the importance of phone numbers. With BYOD, employees own not only their device, but also the phone number associated with it. So when those employees leave the agency, they take those calls and SMS messages with them. Unless former employees are considerate enough to provide callers with a way to reach the agency, constituents will be frustrated that no one is responding. Or worse yet, they might reach out to the former employee directly and may receive information not authorized or sanctioned by the organization.

That's why it's important to look for a solution that can assign a second, work-only number to employee-owned smartphones. When those employees leave, the work numbers stay with the government agencies that issued them. This type of persona-based solution also enables their employers to record and archive only work-related calls and SMS messages, such as for regulatory compliance.

Like their peers in enterprise, government agencies have learned that mobility is a set of challenges and opportunities. In the case of BYOD, one challenge is understanding that a single-OS, hardware-centric EMM solution is no longer a viable way to secure devices, support regulatory compliance, and maximize employee satisfaction. That's why so many government agencies have shifted to platforms that can accommodate the increasingly fragmented OS environment that's now the norm in today's workplace.

Mobile technology also changes rapidly, with OS market shares dramatically rising and falling in popularity, sometimes within the course of just a single year (for example, look at how iOS came out of nowhere to unseat BlackBerry). The same rapid change isn't limited to smartphones, either, as consumers snap up smart watches and other emerging types of wearables. Mobile consumers won't want to leave their favorite gadgets at home, so government organizations will need EMM solutions that are flexible enough to extend security, compliance, and other policies to BYOD. 

Sources

1. Forrester Research, Inc., commissioned by Cisco Systems. BYOD In Government: Prepare For The Rising Tide. Report. October 2012. http://www.cisco.com/web/strategy/docs/gov/cisco_forrester_byod_government.pdf
2. "Bring Your Own Device." The White House. August 23, 2012. <https://www.whitehouse.gov/digitalgov/bring-your-own-device>.

About the Author:

Joseph Petroski is Senior Director of Sales Engineering at CellTrust Corporation. Leveraging over a decade of mobility and sales engineering expertise, Mr. Petroski is responsible for actively driving and managing the technology evaluation stages of the sales process, working in conjunction with sales leadership as a key technical advisor and product advocate on behalf of our customers in financial services, healthcare, government, and large enterprise. Prior to CellTrust, Mr. Petroski held senior sales engineering and product management roles at Vocera Communications and Research In Motion (RIM) Limited, now BlackBerry Limited. Before RIM, he managed and led mobility initiatives supporting critical IT environments at Community Health Systems (CHS).

