PUT YOUR MOBILE STRATEGY TO WORK FOR AGENCY TRANSFORMATION

Federal agencies may already have the tools they need to boost workforce productivity, enhance mission outcomes and improve security

If your agency's employees need to put down their mobile devices to perform tasks on their desktops, it may be time for a mobile reboot.

Agencies and enterprises alike are grappling with what's being hailed as the Fourth Industrial Revolution, where everything will be digitally connected — not just our phones and tablets, but our work environments, our homes, what we wear, even our bodies.

Nowhere has that become more evident than on our smartphones. There are more mobile devices than people in the world, and sensors, wearables, and the Internet of Things will push mobile numbers much, much higher. Chances are high that you and your employees are completely comfortable navigating life around a personal smartphone — more than three quarters of Americans do — using it for everything from reading to connecting with friends to tracking your health.

So why are so many federal agencies still stuck in the PC era, and what's keeping them from capitalizing on the inherent productivity gains that a mobile strategy can provide?

MOBILE MYOPIA

Too often in the federal workforce, "mobile" means remote access to work email and calendars — and stops there. Employees find themselves chained to their desks to perform tasks that they could do faster, more easily and often more effectively using their mobile phones or tablets. Perhaps just as often, business and mission leaders think "mobile strategies" are about the devices, not how business processes and mission operations might be entirely reimagined once employees are untethered from their desks.

Adopting a "mobile first" strategy in the federal government makes sense on so many levels. It embraces the way we live and work in the 21st century. It prepares your agency to step boldly into the future. It offers a proven and economical path toward modernizing IT. And perhaps most of all, it empowers your personnel to work in more flexible and productive ways.

Many agencies and departments, of course, are already seizing a mobile-enabled world of digital opportunities. The Marine Corps' Marine Common Handheld program, for example, has reengineered the way it supports troops' battle readiness by providing military personnel a wide array of mission information on their mobile devices and the ability to update that information in real time.

Other federal agency leaders, CIOs and IT managers, however, are lagging behind. They understand the need to join the "connected" age, but may lack a clear strategy or an agencywide commitment for doing so. While the apparent lack of budget can deter even the most visionary of leaders, the fact is, going mobile can save time and money, and present unprecedented opportunities for innovation — in the office and at the mission edge.

MOBILITY TRANSLATES INTO PRODUCTIVITY AND SECURITY

Where mobile technology is embraced, employees tend to be more engaged. In one study. workers who considered their employers mobile pioneers were more productive — by 16 percent — than those who gave their workplace technologies a low ranking. These workers also scored higher in creativity (18 percent) and were 23 percent more satisfied and 18 percent more loyal. A recent Frost & Sullivan survey commissioned by Samsung supports these findings: In it, 34 percent said using a smartphone for work increases productivity.

But modern mobile devices also give agencies something else: security features that in many cases offer greater data protection than traditional PCs and laptops. Some of these advanced capabilities include derived credentials and biometrics that confirm who is logging in; behavioral authentication for continued verification during use; "containerization" to digitally and physically isolate sensitive work from personal apps; and more.

If mobility makes workers more productive, the inverse is also true: Productivity suffers when organizations fail to equip their people with the tools employees need. That's just one reason why the White House "Report to the President on IT Modernization" specifies mobile technology as a priority. As the report makes clear: "The existing ... approach to IT is no longer sustainable in an increasingly mobile, cloud-based, and complex digital world."

Agencies that have embraced the mobile movement are already enhancing their workers' productivity.

The mobile app for the U.S. Department of Agriculture's Animal and Plant Health Inspection Service, for instance, has dramatically increased the productivity of inspection agents. Using the app on their smartphones, agents can now share information and provide real-time status updates to shippers, importers and buyers. The permitting time reportedly has gone from months to days — and, in some cases, hours — while helping agents focus on more critical tasks.

CAPITALIZING ON THE MOBILE MOVEMENT

A delay in embracing mobile technology comes at a cost. Today's mobile tools allow instantaneous, wireless configurations and customizations that can automatically meet agency specifications the second their users turn them on. That removes a significant burden from IT personnel who performed this task in the past, reduces overall support costs and gives time back to your IT specialists to focus on more critical tasks to the organization. When you start talking about hundreds and thousands of personnel devices, the cost and productivity benefits of enabling simultaneously over the air configuration multiplies exponentially —and becomes a "no-brainer" for federal leaders holding the purse strings.

The hesitancy to adopt modern mobile technologies also presents new risks. Employees, frustrated with aging tools at the office, are literally taking matters into their own hands and using their personal devices and apps for work — creating a growing concern about attacks coming from unsecured devices accessing agency networks.

The good news is, many agencies and departments may already have the mobile device management tools they need to upgrade their capabilities and are just not taking full advantage of them to protect their data, says Craig Ano, leader of federal sales engineering at Samsung Electronics America.

Their devices also may have more capabilities than they realize — with federally approved security features built right into the hardware, for instance.

WHERE TO START

A few simple steps can put federal IT leaders on the right path, including:

1 **Assess your position.** Take an honest gut-check of where you are with mobile technology and the processes your agency needs to support your mission and your employees — now and in the future.

2 **Assess your mobile capabilities.** Take a thorough inventory of the mobile devices and applications already accessing your network — as well as the mobile device management and configuration systems you're already supporting. Determine which devices and apps are most productive for various user groups.

3 **Assess what the market now has to offer.** Mobile devices rival PCs in power, are often more convenient for workers to use and, depending on the models, are even more secure. Samsung Dex, for instance, can run virtualized Windows desktops and enterprise applications using just a Galaxy 8 smartphone and a monitor. And with the embedded Samsung Knox platform, agencies can get Defense Department-grade security that relies on the hardware, not just the software, to protect data even when a device has been compromised.

4 **Assess your risks.** All agencies must determine how best to protect their data and network systems, and to what degree. Rating the risks associated with various users or data, based on NIST recommendations, and applying the proper configurations can help identify opportunities to significantly improve employees' productivity, while keeping mission-critical data secure.

DON'T GO IT ALONE

Of course, conducting these assessments can be difficult for busy IT departments, especially given the rapid pace of technological change. Consider using a trusted partner in the original equipment manufacturer (OEM) community to gain a clearer picture of what technology features are available now — and on the horizon.

OEM's with extensive experience with, and expertise in, government security requirements can point out strengths and weaknesses of various technology features. They also can recommend best practices to improve your mobile strategy while saving money.

It's easier now to centrally configure and control how data is transmitted, contained and used on these devices, says Ano. If you already have these capabilities, your main obstacle to upgrading your mobile strategy may be understanding how to use them. Again, a trusted technology partner can help navigate the possibilities.

Even if your agency performed this kind of analysis a couple of years ago, features and security capabilities have changed significantly, putting agencies in a better position than ever before to secure their data and take bolder steps toward a mobile-first strategy.

The mobile age is maturing quickly. Savvy enterprises in every sector are embracing the future now by optimizing their mobile capabilities environments. With a trusted partner to help assess what you already have and how best to use it, your agency may be able to do so, too, even within the bounds of budgetary and security constraints. Transformation may be much closer at hand than you think. In the Fourth Industrial Revolution, will your agency lead, or lag behind?

Learn more about how Samsung, a leader in government-approved mobile technologies, can help your agency update your mobile environment and make it as safe and secure as it can be — today and tomorrow.

This article was produced by fedscoop | cyberscoop for, and sponsored by, SAMSUNG.