



Federal CIO Insights: What's Next in Mobile Security

sponsored by
 **Lookout**

Political leaders and their policies come and go, but for the federal government, one thing is here to stay: mobility.

Mobile devices started out simply providing email, telephony, and maybe a basic calendar app.

Now mobile devices are full enterprise endpoints, making direct use of networks, using enterprise-deployed applications, and accessing enterprise data. Yet the most widely used mobile devices, running iOS or one of the Android variants, were conceived primarily as consumer devices. Their operating systems and multiple sensors—

Wi-Fi, GPS, cellular—generate location information. Users usually obtain them from carriers' retail stores or manufacturers.

Plus, employees use the devices everywhere, from within highly secure facilities or over virtual private networks. Public retail places providing open, unsecured Wi-Fi makes them vulnerable to, among other dangers, man-in-the-middle attacks in which hackers intercept data in motion without the user even being aware.

Mobile security presents one of the government's biggest information technology challenges.



To explore federal mobility security issues, Federal News Radio convened a panel of federal practitioners:

- David Epperson, chief information officer (CIO) of the National Protection and Programs Directorate at the Homeland Security Department
- Arlette Hart, chief information security officer (CISO) at the Federal Bureau of Investigation
- Jake Marcellus, acting mobility portfolio manager at the Defense Information Systems Agency
- Paul Morris, acting CISO at the Transportation Security Administration
- Retired Army Major General Jennifer Napper, vice president for defense and intelligence at Unisys
- Dr. Leslie Perkins, deputy chief technology officer (CTO) of the Air Force
- Dr. Joe Ronzio, deputy health CTO at the Veterans Health Administration
- Rob Palmer, deputy CTO at the Homeland Security Department
- Bob Stevens, vice president of federal at Lookout.

Hart framed the issue succinctly, pointing out that every device is consumer based, not having been designed for the enterprise. She added, “We can’t find a mobile device management tool with full visibility” into devices and into the insider threat.

That full visibility, IT professionals say, is needed to fully understand what’s on a given device and what it’s doing. Without that view, agencies will have gaps in their ability to ensure secure mobility.

IT shops face what Morris called an escalating threat landscape. It’s expanding in three dimensions.

First, mobile devices are doubling or even tripling device counts, enlarging the so-called cyberattack surface. Plus mobile devices are more prone to loss and theft than larger devices.

Second, unsecure applications reside alongside enterprise ones on a given device. That’s partly because certain public applications have real utility for users, and partly because people expect to be able to use them, especially on devices operating under a bring-your-own-device (BYOD) option. Beyond the indirect threat of sensitive data leaking outside the device container, many commercial apps come from sources that have potentially added malware to the download.

Third, cloud computing blurs the network perimeter, making it more challenging to enforce security policies and keep devices behind the firewall.

Given these conditions, several mobile security challenges have emerged.

...mobile devices are doubling or even tripling device counts, enlarging the so-called cyberattack surface. Plus mobile devices are more prone to loss and theft than larger devices.

Authentication: CAC in the mobile ecosystem


A big issue for federal agencies is ensuring the user is authorized, especially in DoD and national security settings, where the common access card (CAC) doesn't mix well with mobile devices. One promising solution involves putting CAC data onto mobile device SIM cards. Morris of TSA said a pilot program for such credentials is underway.

Also needed: universal federal use of two-factor authentication.

Visibility: MDM is not enough

Visibility into mobile devices with containerization technologies isn't always foolproof. Containers aren't used widely in the private sector in part because they are easily breached. Security managers say mobile device management (MDM) solutions are useful for enforcing policies and tracking devices. They don't, however, provide the level of device visibility that would enable predictive analytics – that is, patterns of usage and behavior that can forewarn administrators of nefarious behavior on a user's mobile device. MDMs also may not detect rogue applications or applications from unauthorized sources that might carry dangerous payloads.

They don't, however, provide the level of device visibility that would enable predictive analytics – that is, patterns of usage and behavior that can forewarn administrators of nefarious behavior on a user's mobile device.



Experts agree their direct security challenge is protection of data, not precisely control of apps or user behavior. After all, it's data that enables mission effectiveness.

Spectrum of Risk: Understanding unexpected threats

Outright malicious behavior is happening, whether on desktop or mobile devices. This behavior can lead to data compromise. Less understood are the inadvertently risky, everyday behaviors that put personal and government data at risk. There is a remarkably wide spectrum of risk through which an individual's or an agency's data can be compromised. People and enterprises need to be informed of these risks and be offered comprehensive solutions that enable them to embrace mobility, with the peace of mind that their sensitive information is protected.

Tool proliferation has created a mobile security challenge as it has for all platforms. Each tool has a useful function, but each produces its own data logs and alerts. Added up they can either overwhelm security staffs or make it difficult to distinguish the truly urgent alerts.

The growth in mobile productivity draws cybercriminals' attention to mobile platforms where they perform increasingly sophisticated attacks. That, coupled with the explosion of mobile apps, exposes agencies to new risks. Some of these risks stem from poorly coded applications and bad app behaviors.

Experts agree their direct security challenge is protection of data, not precisely control of apps or user behavior. After all, it's data that enables mission effectiveness. Many IT shops avoid setups that store enterprise data on mobile devices, or send data to devices for processing.

Still, data is now primarily accessed and transmitted via mobile apps, giving individuals tremendous control over which apps they install for work or pleasure. It lets them control how and from where they access **government** information. The apps themselves and the behaviors they exhibit introduce additional layers of complexity to the mobile ecosystem – another layer of risk that corporate IT and security staffs must address.

Is BYOD really an answer?

Federal security practitioners are not sold on BYOD. At the same time, they understand the unique capabilities for mission requirements these multifunction devices offer. Examples include taking pictures with time, location, and other metadata; and e-mailing them with forms or documents into offices or case management systems.

Managers feel agency-provided devices let them ensure that even commercial or consumer apps come from trusted sources and with configurations that conform to security policies.

Federal technology and security managers are looking for the emergence of several capabilities from mobile security products:

Epperson of NPPD said mobile hypervisors are not adequate to ensure security of data. He said a better approach for some applications is to treat mobile devices as X-terminals or virtual desktops. They display application activity, with the processing of data occurring on remote machines – virtual or physical – within the data center or a secure cloud. Morris added that until total virtualization becomes available, the IT “C” suite will need to remain rational about what users need to do.

- Tools to produce better visibility – or situational awareness – into individual devices at risk.
- Mature integrations between devices and mobile devices, mobile device management systems, mobile threat defense, and existing SIEM systems.
- Detection and remediation of all threats on the Spectrum of Risk including network threats, malware threats, and seemingly benign employee or app behaviors that actually put government data at risk.
- Further down the line, applying security best practices to emerging internet-of-things devices.

As for the management side, they're thinking about:

- A government-wide approach to app vetting to save agencies time and duplicative effort.
- The promise of mobile computing, not letting the risks stop progress. Stevens pointed out mobility is about productivity and morale.
- Risk management for mobility. Epperson says this means learning how to measure mobility risks while maintaining a focus on the mission and data protection.

Palmer of DHS summarized it by asking when the IT community will get away from mobility as something distinct, and begin treating it as just IT, a way people interact with data. Mobile computing has moved quickly to the mainstream. Government has to make sure it has secure mobility.