The MobilityHub
SECURING DATA & APPS.

John Edwards

Mobile Security Lessons From the Military

John Edwards, Technology Journalist, 4/1/2013

As the technology used by military and everyday citizens merges, many of the practices the military uses to secure its data can also be adopted by civilian organizations.

The Department of Defense (DoD), looking to slash costs and equip troops and civilian employees with more modern technologies, is increasingly turning to consumer- and business-type smartphones, tablets, and portable computers. Unlike traditional military communication systems, which generally operate on highly fortified closed networks, the DoD's emerging crop of commercial off-the-shelf (COTS) devices send data over commercial 3G and 4G wireless networks, largely relying on the standard security protections device manufacturers and commercial carriers build into their systems.

As the DoD pushes headlong into COTS technology, it's encountering many of the same data security challenges facing private industry, only on a much wider scale and with the added burden of protecting information that, if exposed, could potentially place troops and/or national security at risk.

Improving device management

At the cornerstone of the DoD's latest mobile security strategy, announced in late February, is an attempt to gain better control over the devices it acquires through commercial channels. To ensure that units are completely secure, the DoD has charged the Defense Information Systems Agency (DISA) with the task of finding mobile device management (MDM) software that's compatible with both iOS and Android devices. As it conducts its search, DISA is looking for MDM tools that, at the very least, allow administrators to remotely manage mobile device software and configurations and offer to ability remotely wipe devices that are lost, stolen or compromised.

Although MDM software is widely available and is relatively easy to deploy and use, a large number of businesses still haven't adopted the technology. That's a shame, since MDM technology is one of the cheapest and easiest ways to protect mobile device-stored business data against multiple security threats. Any business using mobile devices would be smart to follow the DoD's lead in this area.

Opening an app store

DISA is also looking to develop an app store to that would allow DoD troops and employees to safely search for and download enterprise mobile software. The concept is already being tested in a trial project. Last year, the Army launched a pilot version of its Army Software Marketplace. The Army's app store currently contains about a dozen downloadable iPhone and iPad apps, a

number that the Army hopes will grow significantly in the years ahead.

While relatively few businesses have gone to the trouble and expense of opening their own mobile app stores, the concept could eventually turn into a trend with some serious traction. Limiting enterprise mobile device users to internally downloaded apps promises to be an effective way of curtailing malware outbreaks, particularly for companies using Android devices. Many businesses will be watching the DoD's app store experiment with great interest to see how it plays out.

Related posts:

- If It's Good Enough for the Army…
- Mobile Security Advice From the NSA
- Mobile Technology Improves Public Safety