Agencies Continue to Struggle with Gaps in Basic Mobile Security Practices

Posted At : January 29, 2014 10:45 AM | Posted By : Kyra Fussell
Related Categories: Mobility, Technology Trends, Information Security, Cybersecurity, Wireless

A recent report on practices and vulnerabilities, finds room for improvement across the government's mobile security practices.

Mid January 2014, the Mobile Work Exchange published ***The 2014 Mobilemeter Tracker***. The report highlights findings from the **Secure Mobilemeter**, a self-assessment tool for evaluating mobile practices and procedures. End-user and agency data collected through the Secure Mobilemeter during September, October, and November 2013 included responses from 155 individuals and 30 agencies, including the Department of Justice, Homeland Security, Navy, General Services Administration, and Department of Agriculture.90% of individual government respondents indicated using at least one mobile device for work (e.g. tablet, smartphone, or laptop). Nearly 70% use a government-furnished device, 15% use a personal device, and 16% use both.

The report found that while most government employees leverage mobile computing in some capacity, best practices are not followed consistently. Based on the scale devised for the report, 41% of government employees need to improve mobile device security practices. For example, 25% of respondents indicated a failure to secure mobile devices with passwords and 31% accessed public Wi-Fi with a work-related device. Other gaps in basic security include 14% fail to lock their computers when away from their desk. Similarly, 22% of employees do not always store files in a secure location.

Although the Federal Digital Government Strategy has contributed to progress in a number of areas, over 25% of government employees have not received mobile security training. Further, 57% of agencies were found to have gaps in mobile policies and security systems. Agency level vulnerabilities include practices around registering mobile devices with the IT department, utilizing a remote wipe function, tracking phones, and leveraging multi-factor authentication or data encryption.

As government agencies increasing rely on networked systems and mobile computing capabilities, lagging policies and organizational culture pose greater and greater risks to government systems and data. Agencies and vendors must keep pace with new security requirements that emerge from operational shifts driven by advancements in mobile technologies. The push for government organizations to achieve greater operational efficiencies through technology adoption raises the stakes for vendors competing for contracting opportunities, who are tasked with helping agencies close capability gaps and compliance with evolving standards.

---

*Originally published for Federal Industry Analysis: Analysts Perspectives Blog. Stay ahead of the competition by discovering more about **GovWinIQ**. Follow me on twitter **@FIAGovWin**.*