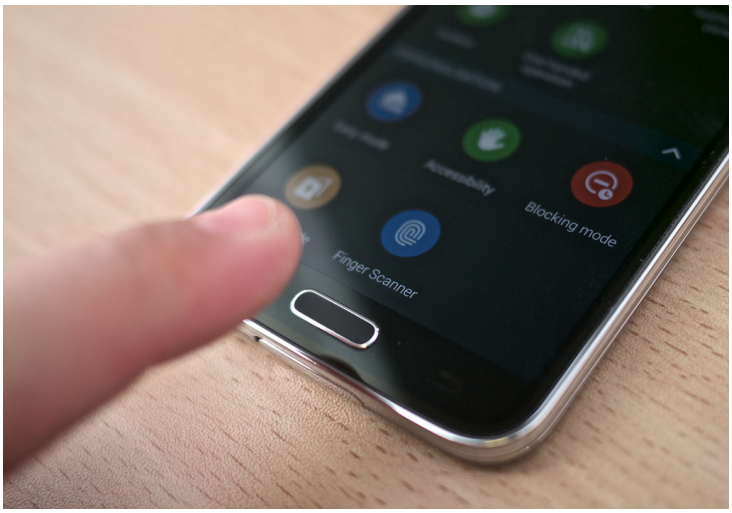
Government Business Council

SAMSUNG

THE TOP 3 CHALLENGES LIMITING MOBILITY IN THE FEDERAL WORKPLACE

TECHNOLOGICAL, CULTURAL, AND BUDGETARY HURDLES ARE STRAINING THE GOAL OF A DIGITAL AND MOBILE FEDERAL WORKFORCE. WHAT IS YOUR AGENCY DOING TO MEET THE CHALLENGE?



Since the 2012 Digital Government Strategy, numerous federal agencies have laid out ambitious plans to accelerate the adoption of mobile technology, both to encourage flexibility and innovative problem-solving among federal employees, as well as to deliver information and services to the American public more efficiently.[1] Yet, the expansion of mobile devices in the federal workplace raises a new host of issues. These issues can be grouped broadly into three categories:

1. **Technological challenges** stemming from the proliferation of mobile malware and other security threats
2. **Cultural challenges** that risk the integrity of mobile data through human error
3. **Budgetary challenges** that limit the choice and scale of mobile technology adoption

To fully realize the benefits of mobile technology, federal agencies will require mobile security solutions that are flexible and scalable enough to meet the diverse needs of the federal workforce, as well as tough enough to safeguard government communications against a broad array of modern threats.

The Technological Challenge

Each day, federal agencies are the target of a wide range of cyber threats directed at their critical networks and endpoints. According to security experts both in and out of government, expanding the number of mobile endpoints could complicate the already difficult task of keeping federal data safe from unauthorized access.[2] Given the persistent threats agencies face, it comes as little surprise that a May 2014 Government Business Council (GBC) survey of federal executives identified security as the primary obstacle to mobile device expansion. In particular, survey respondents raised concerns as to the security of mobile device hardware and software (55 percent), mobile applications (49 percent), and external networks (47 percent).[3]

One of the most unsettling trends for federal leaders in recent years has been the rise in mobile malware, which can be used to steal a user's passwords and sensitive data, track their location, and initiate the download of harmful files, among many other unwanted operations. The GBC study corroborates this trend: two-thirds of federal leaders believe viruses and malware represent a major threat to their agency's data.[4]

One factor likely driving the surge in malware incidents is the popularity of mobile applications that can be downloaded directly onto a user's device – often from untrusted app stores. Of the four million mobile apps tested by cybersecurity experts at Webroot, more than 40 percent contained code that was "unwanted," "suspicious," or "malicious."[5] In addition, experts estimate that anywhere from 60-98 percent of malware incidents target devices that run on the Android operating system.[6] As underscored in Digital Government Strategy Milestone 5.4, federal agencies have an interest in leveraging commercially-available mobile apps as tools to boost innovation.[7] However, mitigating the associated security risks will require technologies capable of both insulating government data from malicious applications, as well as restricting users' access to only those apps available from trusted sources.

The Cultural Challenge

Expanding the safe and effective use of mobile devices in the federal workplace may take a shift that is as much cultural as it is technological, requiring agencies to enact procedures to better manage the ownership of mobile data and limit the risks posed by human error.

Recent studies suggest that human error represents a much greater security threat than previously imagined.[8] A 2014 Mobile Work Exchange study indicates that federal employees frequently engage in risky behaviors like connecting to public WiFi (31 percent), not using password protection (25 percent), and downloading personal mobile applications on their work phones (15 percent).[9] Similarly, GBC found that less than half of federal managers believe that employees receive adequate training in mobile security. It is therefore unsurprising that the majority of respondents consider the loss or theft of mobile devices (66 percent) and unauthorized transfer/disclosure of data (54 percent) to be the leading threats to their agency's data.[10]

"LESS THAN HALF OF FEDERAL MANAGERS BELIEVE EMPLOYEES RECEIVE ADEQUATE TRAINING IN MOBILE SECURITY."

On the other hand, mobile users' privacy concerns represent another major hurdle to mobile expansion, particularly in cases where federal employees use personal devices for work-related functions. For example, to mitigate many of the risks posed by cyber threats and human error, agencies are increasingly turning to mobile device management (MDM) solutions. MDM gives IT officials access to an agency's devices to monitor them for threats and potentially disable specific functions. But as a 2012 Fiberlink survey illustrates, mobile users may be reluctant to consent to MDM on their device if they deem it too intrusive on their privacy: 82 percent are concerned about their employer tracking their web histories during non-work hours, while 86 percent worry about the unauthorized deletion of personal applications.[11] Given these concerns, it is no wonder that 63 percent of federal managers surveyed by GBC believe they need separate mobile devices for work and personal use.[12]

The Budgetary Challenge

The GBC data shows that federal leaders view fiscal constraints as one of the leading factors limiting mobile expansion, second only to concerns over device security.[13] Due to stagnant IT budgets and the rapidly-evolving nature of the mobile device marketplace, many agency leaders have been less than eager to line up for expensive, long-term investments in mobile technology. This has made alternatives to the conventional "government furnished equipment" (GFE) model more attractive choices.

"Bring your own device" (BYOD) policies, those that allow agency staff to use their own personal devices for work, represent a workable, low-cost

option. However, in more secure and sensitive environments, hidden costs can often negate BYOD cost savings, for instance, through the need to invest heavily in MDM or to reimburse employees for using their own devices.[14] Alternatively, the "corporately owned, personally enabled" (COPE) model essentially inverts the BYOD formula: agencies supply and maintain control of the mobile device, while allowing the user to install personal applications from an approved list. COPE is quickly becoming the preferred option in enterprise settings, as it gives leadership greater confidence in data integrity and provides users with the flexibility to use a single device for work and personal functions.[15]

With the introduction of the Managed Mobility Program under GSA's Federal Strategic Sourcing Initiative, agencies can now more easily pool resources to procure commercial mobile devices, wireless services, and even MDM solutions at optimized rates.[16] Managed Mobility gives agencies the flexibility to scale desired MDM capabilities efficiently, either through acquiring COPE devices with MDM pre-installed, or through licensing MDM separately and installing it on users' BYOD devices.

Delivering the Security, Flexibility, and Scalability Your Agency Needs

Before federal agencies can successfully leverage mobile technology to enhance productivity and deliver more innovative services to the American people, adopting a mobile security solution that optimizes security, flexibility, and scalability should be a top priority.

"GOVERNMENT AGENCIES CAN BENEFIT FROM SECURITY FEATURES LIKE MULTI-FACTOR BIOMETRIC AUTHENICATION, FIPS-VALIDATED ENCRYPTION, AND MOBILE DEVICE MANAGEMENT TO COUNTER A DIVERSE ARRAY OF MODERN THREATS."

Government agencies can benefit from Common Criteria-validated solutions that employ security features like multi-factor biometric authentication, FIPS-validated encryption, and mobile device management to counter a diverse array of threats, ranging from mobile malware to electronic eavesdropping to human error. In addition, federal leaders might also consider capabilities like containerization, which creates a secure barrier between parallel personal and work interfaces, to prevent unsecured personal applications from compromising government data, while simultaneously ensuring that users' privacy is protected.

To be sure, federal leaders can improve the quality and coverage of mobile security in their agencies through comprehensive training programs and strategic sourcing. However, technology can play a large role in achieving these goals.

About GBC

Government Business Council (GBC), the research arm of Government Executive Media Group, is dedicated to advancing the business of government through analysis and insight. GBC partners with industry to share best practices with top government decision-makers, understanding the deep value inherent in industry's experience engaging and supporting federal agencies.

About Samsung

Samsung Telecommunications America LLC (Samsung Mobile), a Dallas-based subsidiary of Samsung Electronics Co. Ltd. researches, develops, and markets wireless handsets, wireless infrastructure and other telecommunications products throughout North America. For more information, please visit samsung.com

Sources

1. "Government Use of Mobile Technology: Barriers, Opportunities, and Gap Analysis." Chief Information Officers Council: December 2012 https://cio.gov/wp-content/uploads/downloads/2012/12/Government_Mobile_Technology_Barriers_Opportunities_and_Gaps.pdf
2. "2014 State of Endpoint Risk." Ponemon Institute LLC: December 2013 https://www.lumension.com/Lumension/media/graphics/Resources/2014-state-of-the-endpoint/2014-State-of-the-Endpoint-Whitepaper-Lumension.pdf
3. Government Business Council, "Striking a Balance in Mobile Security." Methodology: GBC deployed a survey to a sample of *Government Executive*, *Nextgov*, and *Defense One* online and print subscribers in April-May 2014. The pool of 318 respondents includes employees at the GS-11 through Senior Executive Service grade levels representing at least 26 different departments and agencies.
4. GBC, "Striking a Balance." 2014
5. "2014 Mobile Threat Report." Webroot: January 2014 http://www.webroot.com/shared/pdf/WR_MobileThreatReport_v4_20140218101834_565288.pdf
6. Amber Corrin, "Mobile Malware Meets BYOD." *FCW*: January 30, 2014 http://fcw.com/articles/2014/01/30/mobile-malware-byod.aspx
7. "Digital Government Strategy Milestone 5.4: Adoption of Commercial Mobile Applications within the Federal Government." Chief Information Officer Council: May 23, 2013 https://cio.gov/wp-content/uploads/downloads/2013/05/Commercial-Mobile-Application-Adoption-DGS-Milestone-5.4.pdf
8. "The Human Factor in Data Protection." Ponemon Institute, LLC: January 2012 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_trend-micro_ponemon-survey-2012.pdf
9. "2014 Mobilometer Tracker: Mobility, Security, and the Pressure In Between." Mobile Work Exchange: January 2014 https://mobileworkexchange.com/our-research/research-detail/4413
10. GBC, "Striking a Balance." 2014
11. Jonathon Dale, "BYOD Beware." *MaaS360*: September 26, 2012. Fiberlink and Harris Interactive study of 2,243 enterprise BYOD users. http://www.maas360.com/maasters/blog/security-information/byod-beware-infographic
12. GBC, "Striking a Balance." 2014
13. GBC, "Striking a Balance." 2014
14. "BYOD and Virtualization: Top 10 Insights from Cisco IBSG Horizons Survey." Cisco IBSG Horizons: 2012 http://www.cisco.com/web/about/ac79/docs/BYOD.pdf
15. Craig Sprosts, "Companies Weigh BYOD vs. COPE, But What Really Protects Data?" *Wired*: May 23, 2014 http://www.wired.com/2013/05/companies-weigh-byod-vs-cope-but-what-really-protects-data/
16. Mark Rockwell, "The Nuts and Bolts of GSA's New Mobile Purchasing Agreement." *FCW*: May 24, 2013 http://fcw.com/articles/2013/05/24/gsa-wireless-details.aspx

Images: Flickr user Karlis Dambrans