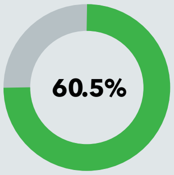
Lookout®

FEDERAL REPORT

Policies and misconceptions:

How government agencies are handling mobile security in the age of breaches

Today's government agencies are embracing mobile security more than ever. Like their private sector counterparts, they realize that whether or not they've experienced a direct threat – which many of them have – now is the time to start protecting data on mobile. Recent high-profile breaches, including the compromise of White House Chief of Staff John Kelly's personal smartphone, have intensified the mobile security focus within state and federal agencies.



of government agencies reported experiencing a security incident involving a mobile device

The results of a recent Lookout survey of government agencies supports this need for urgency. In the survey, 60.5% of government agencies reported they had experienced a security incident involving a mobile device.

Despite the fact that over half of government agencies are experiencing security events via the mobile device, many are still ill-equipped to handle these incidents. Our survey revealed that this may be because many are:

1. Working with outdated assumptions on what constitutes mobile security
2. Bumping up against employee compliance issues with internal policies
3. Unaware of the breadth and depth of their exposure to current mobile risks

Study on Mobile Device Security

April 2017

Science and Technology Directorate

cretary
chnology

, "Study on Mobile
he Department of
with the National
T).
n 401 of the
ppropriations Act of
Stat. 2244, 2977-78

s report is being provided to the following

ot hesitate to contact me.

rt P. Griffin, Jr.
cretary (Acting) for Science and Technology

READ THE BLOG

> "Government mobile devices – despite being a minor share of the overall market – represent an avenue to attack back-end systems containing data on millions of Americans in addition to sensitive information relevant to government functions."

DHS Study on Mobile Device Security, April 2017

DHS recognizes the threat to mobile devices

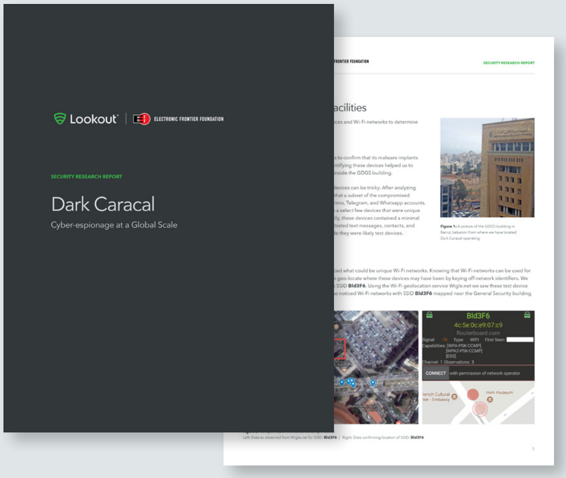
With an increase in mobile advanced persistent threats (mAPT) by state-sponsored actors and other targeted malicious attacks, this renewed attention to mobile security is appropriate and necessary. The stakes are too high to take a wait-and-see approach. The Department of Homeland Security recently published "The Study on Mobile Device Security" highlighting how important mobile security is for our nation's cybersecurity.

Lookout was honored to contribute to this study. The main takeaway is that despite advances, major mobile security gaps remain in the federal government. Closing these gaps as soon as possible is necessary to protect the significant amount of sensitive data and personally identifiable information (PII) held in government systems.

Even the White House isn't safe

The revelation that White House Chief of Staff John Kelly's personal smartphone had been compromised shows how capable malicious actors are at penetrating the highest levels of government. The incident sent enough shock through the system that the White House opted to ban the usage of personal mobile devices in the West Wing.

Microphones, cameras, and the sheer volume of personal and work data accessible on our phones have made mobile devices the ideal weapon for cyber espionage. Using a targeted surveillanceware attack, a malicious actor can control the microphone to listen to private conversations; turn on the camera to take pictures of the surrounding area; or steal information flowing through the device. The recently exposed Dark Caracal mAPT actor and the much-reported Pegasus surveillanceware show examples of such serious mobile spying threats.



Lookout | ELECTRONIC FRONTIER FOUNDATION

SECURITY RESEARCH REPORT

Dark Caracal

Cyber-espionage at a Global Scale

DOWNLOAD REPORT

Yet outdated assumptions about what's "good enough" protection, employee compliance issues, and a lack of full understanding about the risks facing today's government agencies are creating implementation challenges that could threaten national security.

Outdated and faulty assumptions are leaving holes open in the government

96%

have a mobile security strategy

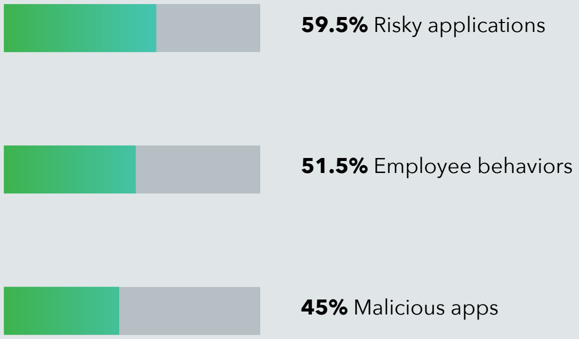
In our recent survey of government agencies, 96% of respondents said their agency had a mobile security strategy, and 94.5% said they are using some sort of management tool, either EMM or Mobile Device Management (MDM).

While this is encouraging, it's only one part of the story. Problematically, 67.5% of our survey respondents said they believe their EMM and MDM security solutions are enough to protect government data from compromise via malicious threats or risky apps/behaviors.

EMM is not a silver bullet, in fact, it's not even a bullet

EMM solutions are important for managing a mobile device fleet, and they enable security by protecting against crimes of opportunity such as targeting an employee that uses an unlocked smartphone, for example. However, EMM solutions alone are inadequate for detecting, analyzing, and responding to mobile attacks.

The following are the top mobile concerns held by government agencies:



While an EMM solution may let an IT manager to wrap a mobile device in a management solution – allowing for the setting of blacklists or whitelists, for example – it is not a solution that provides actionable data and detection of the risks listed above. These three all fall on the Mobile Risk Matrix, which agencies can use as a guide to threats and risks to government data. EMM solutions do not have the data or detection capabilities to keep up with new risky apps employees encounter, potentially harmful employee behaviors, and the constantly evolving threat landscape.

Lookout EMM/MDM partners

Microsoft

MobileIron

BlackBerry UEM

vmware

Workspace ONE™

MaaS360®
by Fiberlink, an IBM company

But it's not only misconceptions about what EMM or MDM solutions can really do that are creating challenges to government security. Employee compliance with existing security regulations can further complicate the effectiveness of standalone solutions.

A mobile security plan is only as good as employee compliance

> "76.5% of survey respondents agreed with the following statement: My employees are willing to sacrifice some government security for the personal convenience of using a personal mobile device for work purposes."
>
> **Lookout Federal Mobile Security Survey,** 2017

When it comes to mobile security, especially when using a standalone EMM or MDM solution, a security plan or policy is only as good as its execution. The results of our survey demonstrate that government employees – like their counterparts in the private sector – are often willing to circumvent internal policy for personal convenience and/or productivity.

As previously noted, 96% of respondents stated that they have a mobile security strategy. Many strategies involve setting a series of policies for employees to follow regarding mobile devices.

Here's what government IT and security professionals had to say about their mobile policies.

Government mobile policies

55% say they do not allow employees to download unapproved apps to their work device

54.5% 54.5% say they require employees to have a pin or passcode for their device

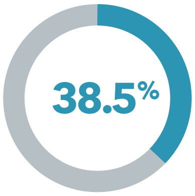
51% say employee must update their device software in a timely manner

45% say employee are not allowed to jailbreak or root their devices

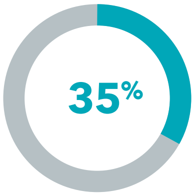
43.5% Employees are not allowed to store work-related information or files on personal devices

40% say employees are not allowed to use personal mobile devices for work purposes

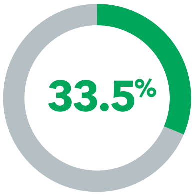
39% say employees are not allowed to take work documents or files home



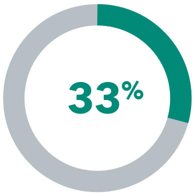
say employees are not allowed to use personal mobile devices for personal purposes while at work



say employees are not allowed to connect the device they use for work to non-government Wi-Fi networks

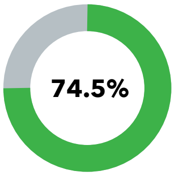
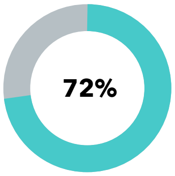
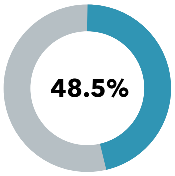
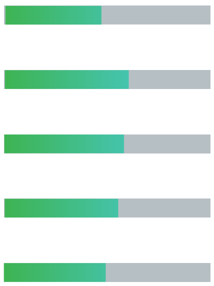


say employees are not allowed to use their work device at home/outside of the corporate network



say employees are not allowed to bring personal devices into the building

The policy, however, does not always match the employee behavior.

Policy	Actual Behavior
Do not download unapproved apps to employee work devices	 of respondents say employees have installed apps to their phone that are not from a major app store
Do not use personal mobile devices for work purposes	 of overall respondents say employees "often" connect their personal devices to federal Wi-Fi for tasks while at work
Do not jailbreak or root mobile devices	 say their employees have rooted or jailbroken a mobile device they use for work
Do not store work-related information or files on personal devices	67.5% say work email is stored on employee personal devices 46% say employees send work documents to personal email accounts
Do not use personal mobile devices for personal purposes while at work	 **46.5%** say employees view/access/send personal emails **60%** say employees use social media apps **58%** say employees send/receive texts **55%** say employees use the mobile browser **50%** say employees take photos

Personal mobile devices are coming into the office, and securing them is a challenge

Enforcing mobile policies when personal mobile devices are coming into the office is not easy. The private and public sectors have this challenge in common: personal devices are a key part of employees' everyday working lives and any security solution needs to work with – not against – this fundamental premise.

When looking at agencies that prohibit personal smartphone use for work,

40% of employees say the guidelines have little to no impact on their behavior

In a 2015 study of federal employees, Lookout found that 40 percent of employees at agencies with rules prohibiting personal smartphone use at work say the guidelines have little to no impact on their behavior. Furthermore, requiring employees to leave work in order to tend to personal business could have a serious impact on productivity – a counterproductive solution when mobile devices are designed to help improve workplace productivity.

Yet in addition to faulty notions of what EMM solutions protect against and concerns about employee behaviors, it's perhaps a lack of awareness of what a comprehensive security solutions needs to include that creates a significant challenge.

What a comprehensive security solution needs to include

We believe that agencies don't have to ban mobile devices to actually gain good security. Mobile threat defense, coupled with mobile management solutions and employee education, provide a solid foundation of protection that enables government agencies to:

- Embrace the digital transformation
- Improve productivity
- Maintain environments employees actually want to work in

The following key capabilities of mobile threat defense include:

- Detection & remediation of the full Spectrum of Mobile Risk including:
  - Mobile malware
  - Compromised operating systems
  - Network-based "man-in-the-middle" attacks
  - Non-compliant/risky apps
  - Risky employee behaviors
- Ease and depth of integration with your Enterprise Mobility Management (EMM), Mobile Device Management (MDM), and Security Information and Event Management (SIEM) platforms

Comprehensive Mobile Threat Defense solutions such as Lookout Mobile Endpoint Security work seamlessly with EMM and MDM platforms to create protections for today's modern government agencies.

Lookout also protects the privacy of employees while still providing the necessary security an agency needs to ensure that government data remains safe. Additionally, Lookout allows administrators to set custom policies against specific employee behaviors (a video is available on that here), so that all employee mobile devices are secure whether they're on the government network or not.

Federal agencies can't afford to wait to secure mobile

With incidents like John Kelly's breach, and the growing mobile threat landscape, it's evident that a mandate for mobile security is coming soon. In time, recommendations from the DHS Study on Mobile Security will likely become requirements, and best practices for securing all the full spectrum of mobile risk may soon become compulsory.

Government agencies will be responsible for implementing and maintaining a comprehensive mobile security plan that secures critical sensitive government data, and protects employee privacy – in the workplace, at home, and while traveling on business.

Fact is, threats and risks exist today – and they are only intensifying in frequency and severity. Agencies that want to stay ahead are getting prepared for the future now.

Interested in learning more ways Lookout can help you secure your agency? Check out our government solutions page.

FedRAMP
In Process

About Lookout

Lookout is a cybersecurity company for a world run by apps. Powered by the largest dataset of mobile code in existence, Lookout is the security platform of record for mobile device integrity and data access. Lookout is trusted by hundreds of millions of individuals, hundreds of enterprises and government agencies, and such ecosystem partners as AT&T, Deutsche Telekom, and Microsoft. Headquartered in San Francisco, Lookout has offices in Amsterdam, Boston, London, Sydney, Tokyo, Toronto and Washington, D.C.

Methodology: The survey was conducted on the behalf of Lookout by Market Cube between October 20, 2017 and November 8,2017 among 200 United States federal IT and security employees.

© 2018 Lookout, Inc. LOOKOUT®, the Lookout Shield Design®, LOOKOUT with Shield Design®, SCREAM®, and SIGNAL FLARE® are registered trademarks of Lookout, Inc. in the United States and other countries. EVERYTHING IS OK®, LOOKOUT MOBILE SECURITY®, and PROTECTED BY LOOKOUT®, are registered trademarks of Lookout, Inc. in the United States. POWERED BY LOOKOUT™ is a trademark of Lookout, Inc. All other brand and product names are trademarks or registered trademarks of their respective holders. 20180207-Lookout-USv1.0