Mobile Work EXCHANGE
Unlocking Productivity

The 2014 Mobilometer Tracker:

Mobility, Security, and the Pressure In Between

January 14, 2014

Mobile Work EXCHANGE
Unlocking Productivity

CISCO

CYBER SECURITY EXCHANGE
MeriTalk

Weather Mapping

According to Cisco's recent Visual Network Index, the number of mobile devices will soon exceed the world's population and by 2017, expect more than 10 billion connected mobile devices.*

The question is – how secure are we with these mobile devices? In conjunction with Cisco, Mobile Work Exchange developed the **Secure Mobilometer**, a self-assessment tool to better understand mobile security best practices and vulnerabilities. The Secure Mobilometer captured data from end-users and agencies, and used a weighted scale to rank their mobile security habits based on user inputs such as password protection, data loss prevention, mobile device policies, and IT and security training.

The 2014 Mobilometer Tracker: Mobility, Security, and the Pressure In Between study highlights the most critical findings of the Secure Mobilometer and offers recommendations to individuals and organizations on what steps to take to address mobility pitfalls and ensure future security.

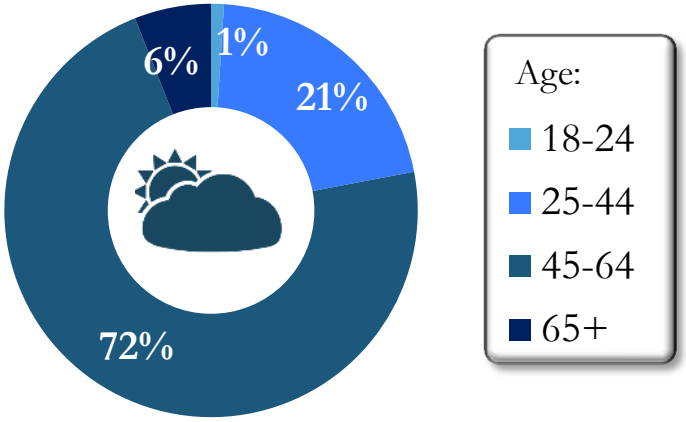
For the purposes of this study, "mobile device" refers to a tablet, smartphone, or laptop.

**Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012–2017 http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html*

Methodology

- Mobile Work Exchange invited government individuals and agencies to measure their secure mobility pressure with the Secure Mobilometer during the months of September, October, and November 2013. This report reflects the calculator inputs of 155 individual responses and 30 agency responses

Individual Responses: **97%** from civilian agencies and **3%** from DoD agencies

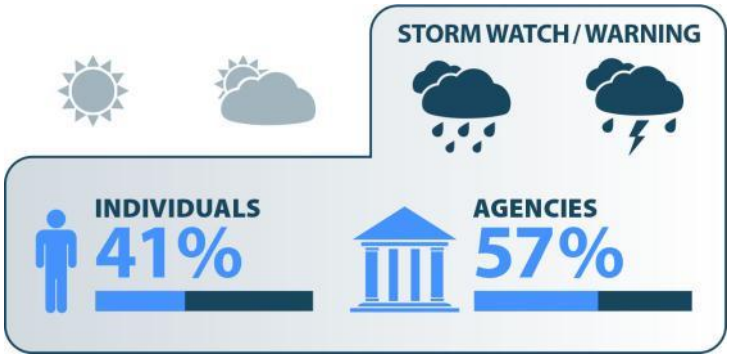


Agency Responses: **90%** from civilian agencies and **10%** from DoD agencies, including responses from:

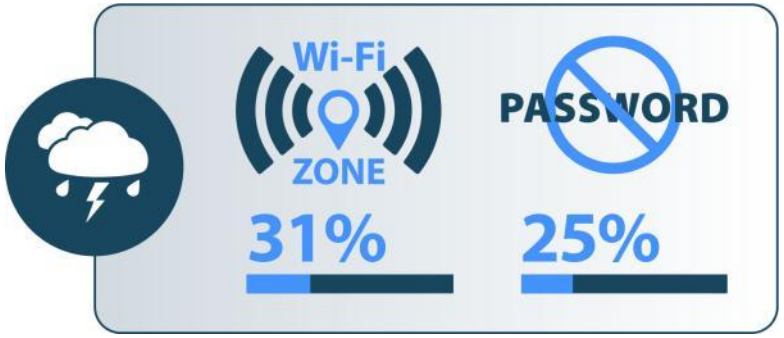
According to individuals, **90%** of government employees use at least one mobile device for work purposes: (**69%** use an organization-provided device; **15%** use a personal device, and **16%** have both)

Mobile Work EXCHANGE
Unlocking Productivity

On the Radar



Storm Brewing: While 90% of government employees are mobile, many individuals and agencies are disregarding security best practices



Thunder Rolls: Potentially dangerous behaviors include public Wi-Fi use (31%) and failure to use passwords (25%)

Why Heed the Warning? 6% of those who use a mobile device for work say they have lost or misplaced their phone

Silver Lining: Government employees scored considerably safer than their private-sector counterparts. In a world where IT leaders must support users' private devices, security becomes paramount, and 15% of government respondents have downloaded a non-work-related app onto the mobile device they use for work vs. 60% of private-sector respondents

*Based on the size of the average Federal agency

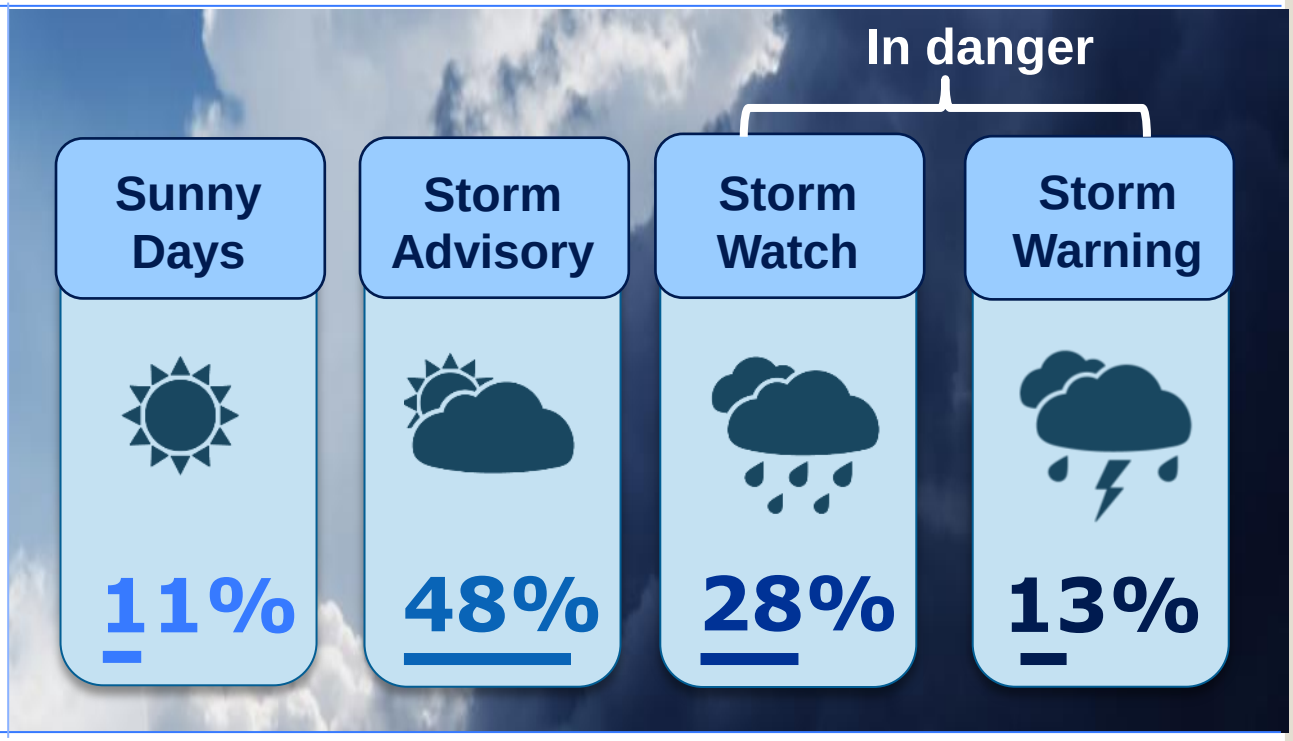
Individual Mobilometer Forecast

Take Away: **41% of government employees need to reevaluate their mobile device security behaviors**

Just **11%** of government employees are in the clear.

48% are mindful of security, but have some low-risk habits to correct.

Unfortunately, that leaves **41%** in the latter categories who are putting themselves and their agencies at risk.



Where are government employees falling short?

Take Away: **Many government employees are taking *basic* steps to secure agency data and devices on the go**

86% lock their computer when they leave their desk

86% have a safe and alternative work place compatible for work

78% say they always store files in a secure location

Storm Warning

Take Away: **Employees' lack of data encryption plus ad hoc behaviors such as public Wi-Fi use and personal app downloads still put agencies at risk**

31% report using public Wi-Fi on a work-related device

15% have downloaded a non-work-related app onto the mobile device they use for work

52% fail to use multi-factor authentication or data encryption

10% have opened an email or text from someone they don't know

Strong Winds Ahead

Take Away: **Many also fail to realize the importance of strong passwords**

One out of four employees

(25%) do not use a password on the mobile device they use for work-related tasks

Even when they do, nearly **one in three** (28%) admit to having used an "easy" password

The most common?

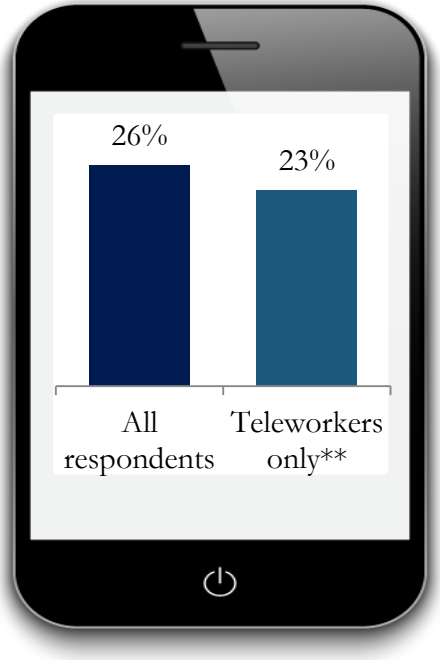
- "Password"
- "1234"
- User's name
- User's initials
- Social security # and birthdate combination

6% have their mobile device password written down!

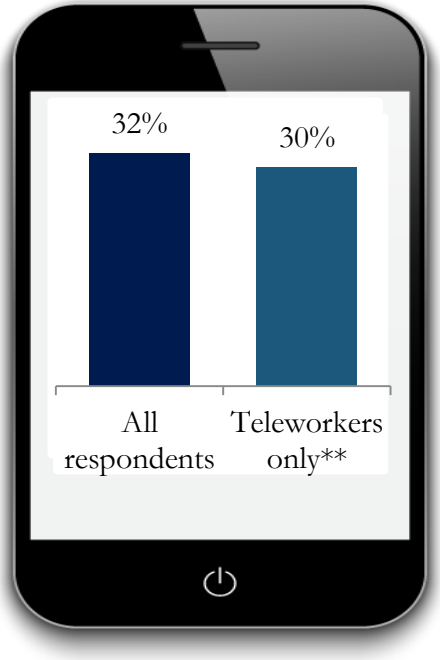
Preparedness Gap

Take Away: **Despite Federal Digital Government Strategy* efforts, more than one in four employees have not received mobile security training. Surprisingly, having a formal telework agreement has *little to no* impact on training**

Percentage of respondents who have **not received security training** for mobile devices



Percentage of respondents who have **not received IT training** to work remotely



* http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html#milestone-6-2 **Those with a formal telework agreement in place

Why Heed the Warning?

Take Away: **One misplaced phone can put an individual, department, or entire agency at risk**

6% of government employees who use a mobile device for work say they have lost or misplaced their phone

In the average Federal agency, that's **more than 3,500 chances** for a security breach*

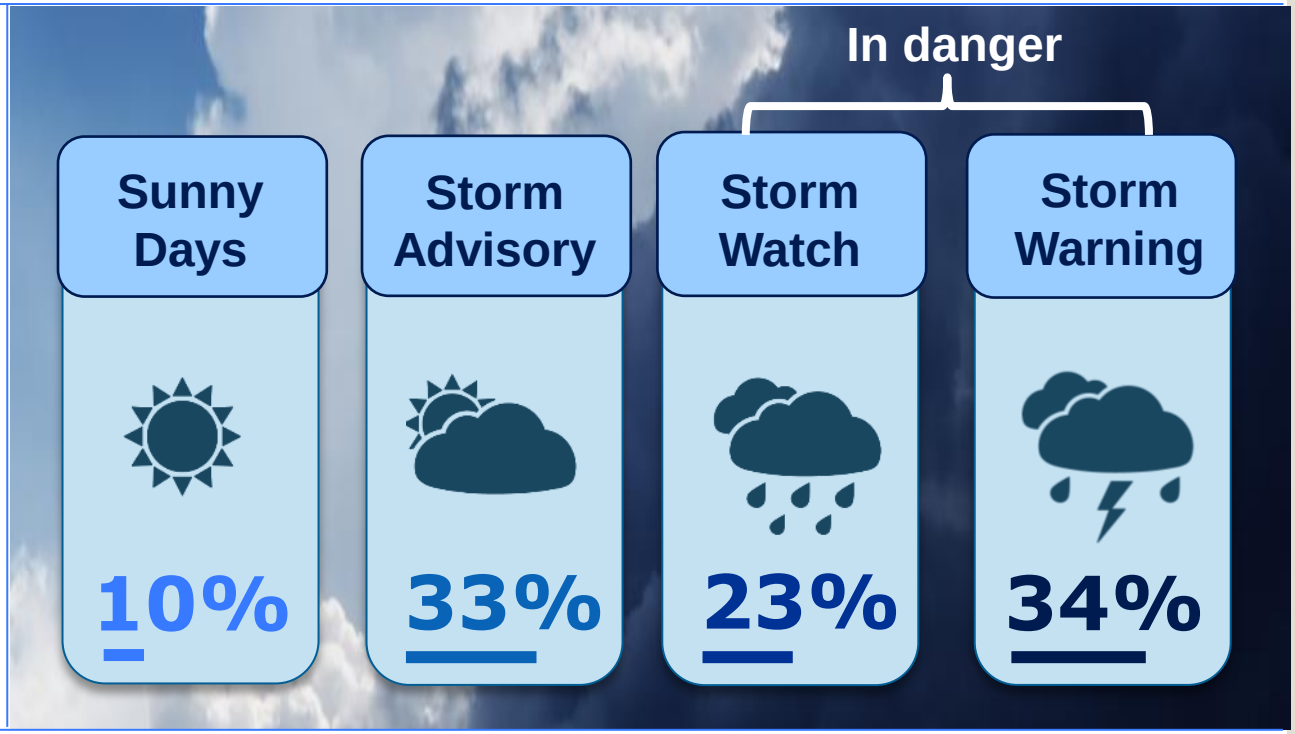
*Estimated number of Fed employees in 2013 across 35 agencies is 2,110,000; which equates to approximately 60,290 Feds per agency. 6% x 60,290 = 3,617. Source: http://www.whitehouse.gov/sites/default/files/omb/performance/chapter11-2013.pdf

Agency Mobilometer Results

Take Away: **Few agencies* offer shelter from the storm**

Just **10%** of government agencies are in the clear.

The majority – **57%** – are failing to secure agency data with gaps in mobile policies and security systems.

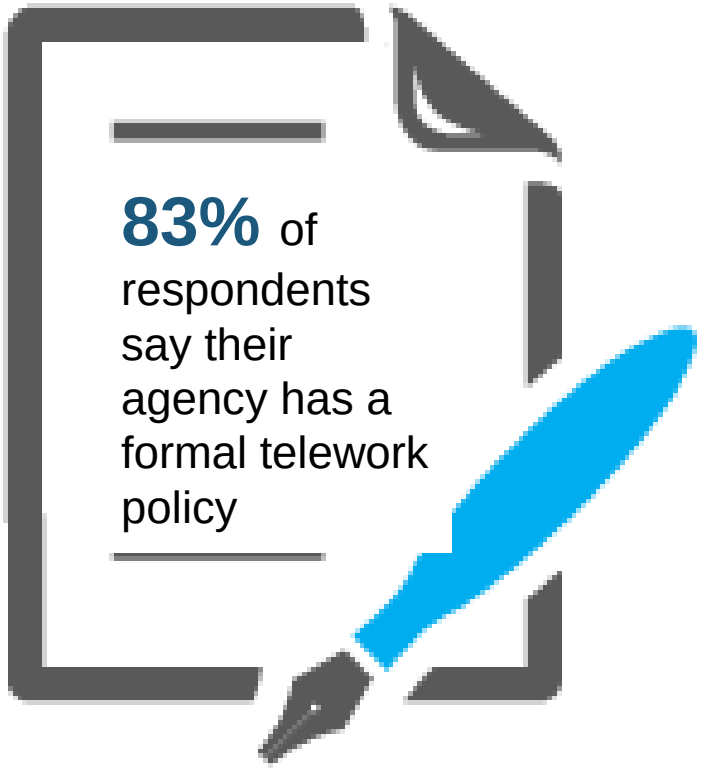


Where are agencies falling short?

*Representatives answering on behalf of their agency

Cloudy Policy

Take Away: **Agencies tackle telework, but miss opportunities to support broader mobility**



But, despite 90% of government employees saying they use mobile devices for work*, just:

50% say their agency has a formal employee-focused mobile device program

57% say their agency provides written mobile device security information to employees

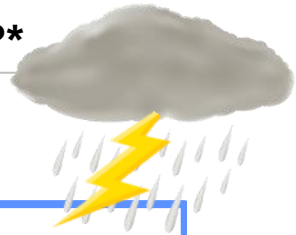
53% say their agency requires employees to take regular security training related to mobile devices

*According to the Individual Mobilometer

Dark Skies Ahead

Take Away: **Just half of agencies report taking fundamental secure mobility steps**

Which of the following secure mobility steps does your agency take?*



Requires employees to register mobile devices with the IT department

53%

Utilizes a remote wipe function on mobile devices

53%

Tracks phones if lost

50%

Utilizes multi-factor authentication or data encryption on mobile devices

47%

*Respondents asked to select all that apply

Mapping Public Versus Private Users

Take Away: **While the government sector still has a ways to go, employees scored considerably safer on the Secure Mobilometer than their private-sector counterparts***

Know your workforce:

97% of government individuals who telework say they have a formal telework agreement in place vs. just **56%** of private sector individuals

Minimize risks:

15% of government individuals have downloaded a non-work-related app onto the mobile device they use for work vs. **60%** of private sector individuals

*According to 97 individuals from the private sector

Mapping Public Versus Private Organizations

Take Away: **Despite shortfalls, government agencies also out-scored private-sector organizations.* What can organizations learn?**

Know your devices:

53% of government agencies require employees to register mobile devices with the IT department vs. just **21%** of private-sector organizations

Require training:

53% of government agencies require all employees to take regular security training related to mobile devices vs. just **13%** of private-sector organizations

*According to 24 organization responses from the private sector

Tomorrow's Forecast: Be Prepared

For individuals:

1. Always use a password on all mobile devices. Make it complex and change it often
2. Always use a secure wireless connection
3. Never open an email or text from someone you don't know
4. Do not store personal info – address, credit card number, etc. – on a mobile device
5. Adhere to security and IT training provided by your organization

For organizations:

1. Establish a formal employee-focused mobile device program, including written mobile device security policies
2. Create regular training and require all employees to participate in training
3. Require all devices to utilize a password
4. Install multi-factor authentication or data encryption on mobile devices to secure organization data
5. Implement a remote wipe function for lost or stolen devices

Thank you.

Cindy Auten
cauten@mobileworkexchange.com
(703) 489-1185

Whitney Bell
whewsonbell@mobileworkexchange.com
(703) 883-9000 ext. 130