MOBILE SECURITY

# Fixing the Disconnect Between Employer and Employee for BYOD (Bring Your Own Device)

WEBROOT®
Smarter Cybersecurity™

## INTRODUCTION

It's no surprise that there are many articles and papers on Bring Your Own Device (BYOD) that will advise employers on how to secure employee devices. With the exponential growth in malware and potentially unwanted apps (PUAs) during 2013, particularly on the Android™ platform, the stakes and risks have never been higher.

BYOD security management adds complications that businesses have not faced before – the devices are owned by employees and contain the owners' personal data.

Webroot believes there is a large disconnect between how employees are using mobile security and the ways that organizations are implementing BYOD. Before conflicts start to erode the considerable gains BYOD brings to both parties, we are uncovering the realities of this disconnect to better inform employers on how to work with employees using personal or employer issued devices.

To explore this disconnect, Webroot commissioned a two part research survey looking at employee and employer BYOD attitudes and concerns around securing personal mobile devices. The first survey took place in late 2013 and explored what employees want out of BYOD, while the second survey, conducted in March 2014, looked at what employers want for securing mobile devices.

While there are some striking areas of agreement, there are also signs that many employees do not take adequate steps to protect company information, a weakness that could result in critical security breakdowns. There is also evidence that employers often only pay lip service to consulting with employees over BYOD security. This can create problems given the large number of personal devices being used for work purposes.

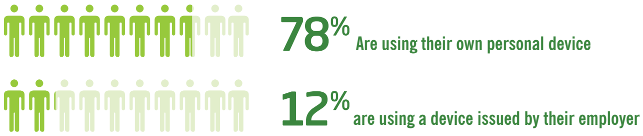
As a result of these research surveys, Webroot has developed an employee BYOD Bill of Rights. This tool serves as a guideline employers can use to help bridge the security gap between employees' preferences and the security requirements of their organizations.

# KEY FINDINGS FROM THE EMPLOYEE BYOD SURVEY

## Mobile Device Usage at Work

Among the over 2,100 individuals surveyed, 41% indicated they use a smartphone or tablet for work purposes (accessing corporate email or other company data).

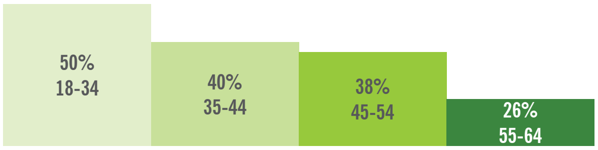
**Of those using a mobile device for work:**



This shows the use of mobile devices in the workplace is overwhelmingly driven by BYOD. Introduction of new consumer devices and declining prices have increased the penetration of personal mobile technology and these devices are being brought into the workplace.

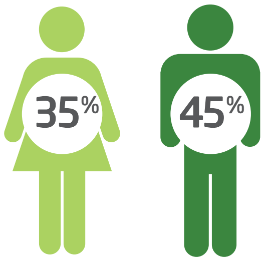
When reviewing the age groups of employee survey respondents, it was no surprise that the youngest group, 18-34 year-olds, is more likely than other age groups to use smartphones/tablets for work, regardless of whether they are personal or employer-issued devices.

**Percentage of work device usage by age demographic:**



When we looked at the gender of the respondents, males are more likely than females to use smartphones/tablets for work purposes.

Male employees are also twice as likely as female employees to use an employer-issued smartphone for work purposes - 14% versus 7%. When it comes to mobile device usage for work, we see that usage decreases with age and is twice as high for 18-34 year-olds versus 55-64 year-olds, but all age groups are using mobile devices for work. And, when you look at BYOD, twice as many mobile devices are now personally owned compared to being company owned—as most devices were just a handful of years ago.

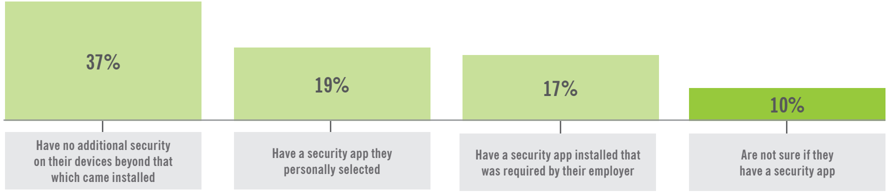


**70%** of employee devices only have the security installed from when the device was purchased.

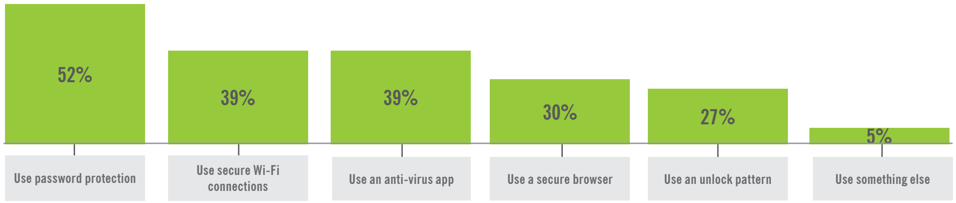
## Mobile Security Installed

When it comes to employee usage of smartphones or tablets for work purposes, 67% of respondents have a security app installed.

### Of that 67%:



### Overall, 86% of those surveyed indicated they've taken some security measures, which included:

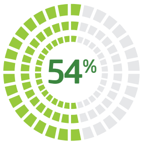


The bottom line is that most employee devices are lacking real security with only 19% installing a full security app and 64% of employees limited to using only the security features that came with their devices. As a result, a priority for employers must be to get employee devices used for work adequately secured and protected.

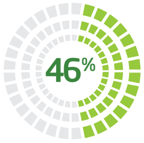
## Attitude Toward Security

Recognizing the need for employees to use secure devices, the survey asked for respondents' reactions to mandated corporate security policies that would require a security app to be installed on personal devices used for work.

Opinions are divided when employees are presented with the idea of a company-mandated security app being added to their personal device. The fact that 46% of employees would stop using personal devices for work creates a potential productivity loss that employers need to address.



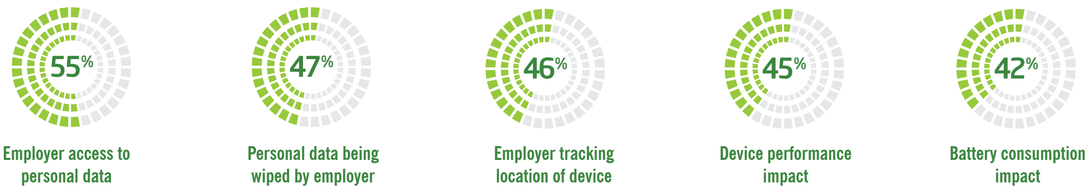
Allow them to install and keep using the device for business purposes.



Stop using the device for business purposes.

## Employee Concerns over Mandated Security

The survey also inquired to see what concerns employees would have about an employer security app being installed on their personal device. Employees who were extremely or very concerned expressed these top issues:

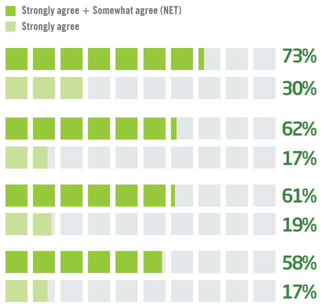


Again, gender differences were evident in this area as 57% of women described themselves as either extremely or very concerned about personal content versus only 41% of men.

These legitimate and important concerns employees expressed over personal data and privacy need to be considered when employers mandate security technology on personal devices if they are to avoid losing the 46% of users who said they would stop using their devices for work.

## Employee Attitudes to Security

Given the high level of awareness around security these days, employees did understand both sides of the BYOD security dynamic. They strongly or somewhat agreed on the following:



I think employees should have some influence on the decision for what kind(s) of software or security is put onto their personal smartphone or tablet that they use for work.

My company has the right to put a security app(s) on my device as a condition of allowing access to corporate data.

If my company requires I have security app(s) on my personal device, I trust our IT security experts will select the best one(s).

I feel I have adequate knowledge of mobile security apps to make a decision about the right solution for me.

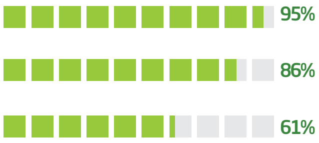
However, it's also worth noting that employees indicated that having some influence on such decisions is more important than the employer's right to install security apps.

Gender differences were also noted in this category. Women were more likely than men to agree that employees should have some influence on the decision for what kind(s) of software or security is put onto their personal devices for work purposes, 84% of women compared to 66% of men.

64% of men indicated they have adequate knowledge of mobile security apps to make a decision about the right solution for them compared to just 49% of women.

## Mobile Device Usage at Work

When employers were asked about mobile device use at work, respondents indicated:



95% Have employees using mobile devices, leaving only 5% not using mobile devices

86% Of employees use company-issued mobile devices
75% using smartphones / 66% using tablets

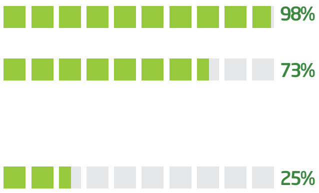
61% Have employees using personal mobile devices
57% using smartphones / 44% using tablets

This indicates a high usage of both company-issued and personal devices at the same time, with company-issued still outpacing BYOD. However, BYOD use is high and well represented.

**98%** of employers have a mobile security policy in place for access to corporate data.

## Employers Mobile Security Policy

Employers were also asked what security they enforced at work when mobile devices were accessing their network for corporate information



98% Have a security policy in place

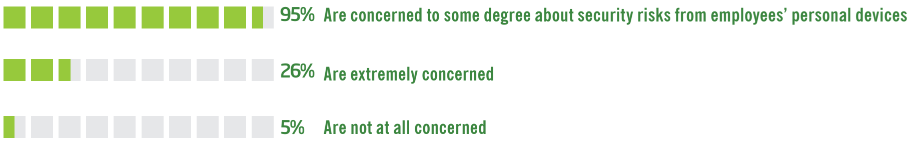
73% Have a policy that allows for personal device access to some degree
- 33% requires a specific IT-mandated security app
- 21% allow personal device access with no security
- 19% require employees to install a security app before any access is allowed

25% Have a no personal device policy, but
- <19% are able to enforce this
- 6% say it is not enforceable

It is heartening to see that 98% of employers have a security policy in place and that 73% allow for personal mobile devices to some degree. Worrying, however, is that 21% allow access with no security at all.

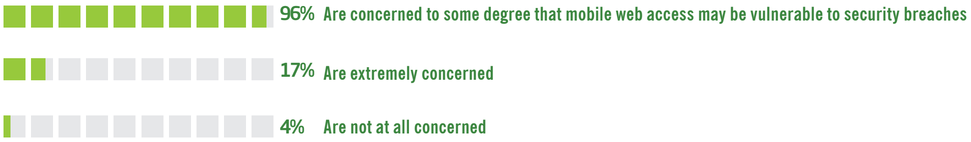
## Employers Security Concerns

Employers indicated their major security concerns when it comes to the use of employees' personal devices to access the company network.



The data risk concern here is considerable and entirely understandable.

Employers were also asked about mobile device access to company based systems using their web browsers and any concerns they had about being vulnerable to security breaches. The results were similarly high:

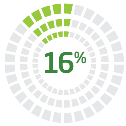


## Removing Security without Wiping Personal Data

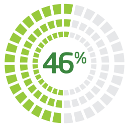
Another aspect of mandating security for work purposes is the employers' confidence that they can remove their mobile device security software on the employee's device without wiping, or causing the user to lose access to their personal data.

These results are the reason employees are nervous about having a company-implemented solution installed on their personal devices. In the employee survey, 47% of employees were extremely or very concerned that the personal content on their devices would be "wiped" if they left the company. The confidence to not wipe users' personal data needs to be much higher.

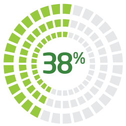
Again, gender differences were also evident related to wiping concern levels. The concern is especially strong among women with 57% describing themselves as either extremely or very concerned, while only 41% of men express the same concern.



Are extremely confident



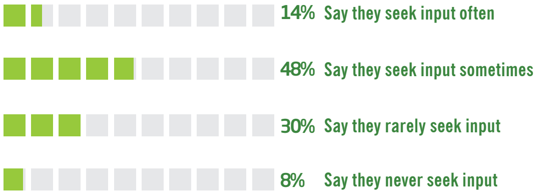
Are very confident



Are somewhat or not confident

## Employee Security Input on Personal Devices

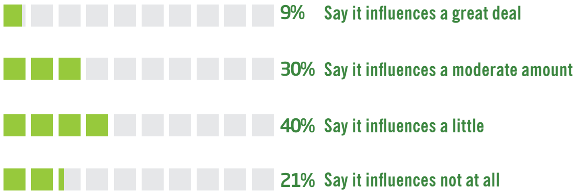
As BYOD devices are owned by the employee, employers were asked how frequently they seek employee input when developing security policies for personal devices.



While it is good to see that most employers seek employee input at least some of the time, it is also apparent that employee input is really not an employer focus, even when they don't fully own either the device or the data in question.

## Influence of Employees on Security Decisions

While 73% of employees expressed that they should have some influence on decisions regarding what kinds of software or security is put onto their personal devices, employers revealed how much influence employee preference has on mobile security decisions.



With 79% of employers indicated employee preference influences security decisions to some degree, these responses align well with employees wanting to be involved. However, the survey reveals that 61% of employers don't really take employee preferences on security decisions into consideration.

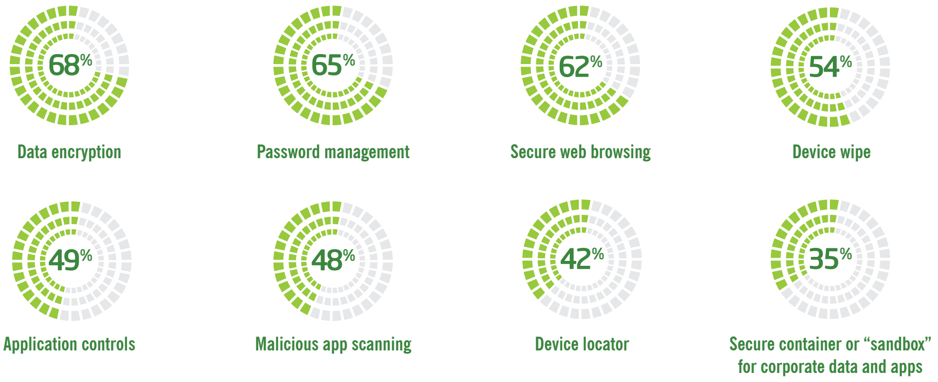
## Essential versus Used Employer Mobile Security Feature Preferences

Given the high level of employer concerns over personal devices accessing the network, employers view the following as the essential security features and also outlines what features they currently use.

This list shows what  employers want from their mobile security in green, versus what they actually use in blue.

What it shows is that the gap between these two, Essential versus Current, is very small—which is a good thing.

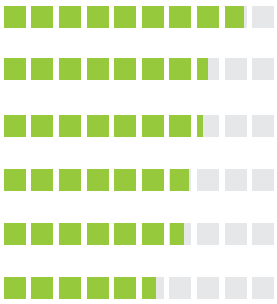
The essential employer security features are:



A significant difference does exist between the "essential" and "actual" for secure web browsing, which may explain some of the high concern employers feel regarding personal devices accessing corporate sites via their web browsers.

## Employer Mobile Security Management Preferences

The employer mobile security survey concluded by looking at employer preferences for operating security on personal devices. The results showed:



88% Preferred to manage mobile security in a common endpoint management environment

74% Agreed that involving employees is a good way to improve security compliance

72% Agreed that allowing employees to use different security solutions is too time-consuming

69% Agreed that they try to include employees in the mobile security decisions

66% Agreed that potential productivity increases from personal devices outweighed risks

57% Agreed employees have enough knowledge of security apps to make decisions about the right solution themselves (This aligns very closely with employees, as 58% thought they had enough to make the right solution decision for themselves)

So, it is clear from the questions we have asked, both of employers and employees, that there are some very interesting dynamics at play when it comes to mobile security on personal devices.

## THE EMPLOYEE BYOD BILL OF RIGHTS

Looking at this from the employee device and personal data owner perspective, some very clear lines of engagement and acceptability between employee and employer have emerged. As a result, Webroot has created an employee BYOD Bill of Rights. This tool acts as a guideline that will help to bridge the gap between employees' preferences and the needs of the employer organization.

1. Privacy over their personal information
2. Be included in decisions that impact their personal device and data
3. Choose whether or not to use their personal device for work
4. Stop using their personal device for work at any time
5. Back up their personal data in the case of a remote wipe
6. Operate a device that is unencumbered by security that significantly degrades speed and battery life
7. Be informed about any device infections, remediation, or other activity that might affect their device's performance or privacy
8. Download safe apps on their personal device

As a result of this research, it is evident that for BYOD to be a success, all employees should have these rights in regard to their personal devices when used for work.

## IN CONCLUSION—FIXING THE DISCONNECT

From the results of these employee and employer research surveys, it appears that most disconnects over the use of personal technology to access corporate data can be solved by better communication between both parties regarding security, data, and privacy concerns.

There are also some very clear recommendations when it comes to BYOD.

» Employees must have mobile device security, and employers need to ensure they install adequate protection and require features like password access are always turned on

» Invest in educating employees about the risks associated with mobile devices and the benefits of securing devices. An informed user is more likely to buy into BYOD security requirements

» Don't mandate security solutions without engaging users first – otherwise employers risk losing productivity from nearly 50% of employees

» Acknowledge the employee's BYOD concerns and personal privacy when setting mobile security policy by using a framework such as the "BYOD Bill of Rights"

» Ensure browser data security breach concerns are answered to the organization's satisfaction

» It's great to have policies, but they only work and are respected if they are enforced

» Simplify management, letting employees choose different security is "time consuming"

Finally, if you don't respect your employees' personal device rights, then they'll simply stop using their personal devices for work, which results in everyone losing the productivity and work-life balance that mobility brings.

## SURVEY METHODOLOGY FOR IT PROFESSIONAL SURVEY

The IT professional survey was conducted online within the United States by Harris Poll on behalf of Webroot from March 31-April 11, 2014, among 205 U.S. adults ages 18 and older, who work full-time as an IT professional in a company with 500 or more employees and have at least a major influence in decision making for mobile device security solutions.

## SURVEY METHODOLOGY FOR EMPLOYEE SURVEY

The employee survey was conducted online within the United States by Harris Poll via its QuickQuerySM online omnibus service on behalf of Webroot from December 13-17, 2013, among 2,129 U.S. adults ages 18 and older, among whom 937 indicated being employed full or part time.

Both of these online surveys are not based on a probability sample and therefore no estimate of theoretical sampling error can be calculated.

**About Webroot**

Webroot provides Smarter Cybersecurity™ solutions. We provide intelligent endpoint protection and threat intelligence services to secure the Internet of Everything. By leveraging our cloud-based collective threat intelligence platform, computers, tablets, smartphones, and more are protected from malware and other cyberattacks. Our award-winning SecureAnywhere™ intelligent endpoint protection and BrightCloud® threat intelligence services protect tens of millions of consumer, business, and enterprise devices. Webroot technology is trusted and integrated into market-leading companies including Cisco, F5 Networks, HP, Microsoft, Palo Alto Networks, RSA, Aruba and many more. Webroot is headquartered in Colorado and operates globally across North America, Europe, and the Asia Pacific region. Discover Smarter Cybersecurity solutions at webroot.com.

**World Headquarters**
385 Interlocken Crescent
Suite 800
Broomfield, Colorado 80021 USA
+1 800 772 9383

**Webroot EMEA**
6th floor, Block A
1 George's Quay Plaza
George's Quay, Dublin 2, Ireland
+44 (0) 870 1417 070

**Webroot APAC**
Suite 1402, Level 14, Tower A
821 Pacific Highway
Chatswood, NSW 2067, Australia
+61 (0) 2 8071 1900