# Boosting Mobile Security and Awareness Reduces Risks

**By**

**Elissa Doroff, XL Catlin**

11/18/2015



Mobile devices have quickly become an integral part of our daily lives.

From everyday social interaction to corporate activity, we spend more time on our mobile devices than nearly anything else—and a significant amount of that time using apps. In fact, according to a report published earlier this year by cyber security firm FireEye, in 2014, mobile app usage accounted for 86 percent of time spent on mobile devices, up from 80 percent the year before. [1]

Mobile devices contain our most personal information, including our calendar, email contacts, photos, videos, music preferences, employer details, credit card information, and more. And yet, in spite of this, most mobile devices lack the security to ensure that they, and the information they contain, are secure.

The FireEye report found that two main platforms dominate the mobile market today: Google's Android and Apple's iOS. Interestingly, the report found that most mobile malware targets Android (96 percent of the time), and that these threats are only increasing.

Android malware surged from roughly 240,000 unique samples in 2013 to more than 390,000 in just the first three quarters of 2014. Apps to steal financial data were particularly prevalent: FireEye saw more than 1,300 unique malware samples in December 2013, compared with just 260 in June 2013.

In addition, more than 5 billion downloaded Android apps are vulnerable to remote attacks largely because of the Google Android platform, which contains many more vulnerabilities that attackers can exploit. Specifically, FireEye reported that the JavaScript-Binding-Over-HTTP (JBOH) may be the riskiest, as it enables attackers to hijack the HTTP traffic to inject malicious content and gain full control of the app running on the device.

Perhaps most troublesome, however, is that, for the majority of individuals using these devices, even the most basic level of security has not been implemented, thereby placing all of their personal and sensitive data at risk.

As further evidence of this trend, according to Ponemon Institute's *Security Impact of Mobile Device Use by Employees* report, published in December of 2014, only 20 percent of employees say they have been trained on mobile device security. Of those, 74 percent think the training was ineffective in reducing security risks.

Because contemporary mobile devices are as sophisticated and connected as any personal computer or laptop, many of the same safety precautions should be taken on them. The National Institute of Standards and Technology (NIST) sets forth guidelines for mobile device security and considers them equally important to a company's privacy policy.

NIST instructs companies to formalize a mobile device security policy that specifies the following:

1. Which types of mobile devices are permitted to access the organization's resources
2. The degree of access that various classes of mobile devices may have
3. How provisioning should be handled
4. How the centralized mobile device management servers are administered
5. How policies in those servers are updated

Businesses also need to develop threat models for mobile devices as well as the information or other resources that are accessed through the devices. These devices often need additional protection because of their higher exposure to threats than other client devices, such as desktops and laptops.

According to the Ponemon study, "employees are clueless about the risk of using mobile devices."[2] Specifically, 66 percent of respondents in the study say that they have either frequently (23 percent) or sometimes (43 percent) downloaded and used mobile apps that do not have the approval of their company.

Should a company-issued device be compromised, thereby enabling an access point to the corporate network, a cyber liability policy could respond.

**Careful Assessment**

Companies should consider both the benefits and detriments of each company-provided device and determine which services are essential for each employee. Categories of services to be considered include general policy, data communication and storage, and user and device authentication and application.

As with all devices connecting to a corporate network, a mobile device solution should be implemented and tested before it is put into production. Each type of mobile device should be evaluated for connectivity, protection, authentication, application functionality, solution management, logging, and performance.

The revised guidance from NIST also recommends that organizations periodically perform assessments to confirm that their mobile device policies, processes, and procedures are being followed properly. Assessment activities may be passive, such as reviewing logs, or active, such as performing vulnerability scans and penetration testing. Companies should also consider a potential risk transfer in the form of cyber liability insurance. Should a company-issued device be compromised, thereby enabling an access point to the corporate network, a cyber liability policy could respond.

Before allowing users to access them, organization-issued mobile devices should be fully secured. This ensures a basic level of trust in the device before it is exposed to threats.

As with any newly implemented policy, companies should regularly maintain mobile device security, including checking for upgrades and patches and acquiring, testing, and deploying them; ensuring that each mobile device infrastructure component has its clock synced to a common time source; reconfiguring access control features as needed; and detecting and documenting anomalies within the mobile device infrastructure, including unauthorized configuration changes to mobile devices.

**Training the First Line of Defense**

Perhaps the most important element in a company's mobile security strategy is the company's employees. Employees are the first line of defense in online security, whether a device is mobile or hardwired.

It is important to provide training to raise employees' security awareness about the risks of potentially compromising any information contained on the device as well as the device itself. For instance, security issues often arise if employees disable security features, download mobile malware, violate corporate data policies, or fall victim to mobile phishing attacks.

Some organizations are stepping up efforts to address mobile device security issues such as installing tracking/wiping software and encryption. Having the appropriate programs installed, however, does not mean they will be used appropriately. The continued challenge with remote wipe policies is that employees highly value the personal data on their mobile devices, but undervalue the business data on those devices. Despite the risks, they do not use the wiping software for fear of losing their personal photos or other noncorporate data.

Recent polls by cyber security firm Centrify[3] and Absolute Software[4], a company that provides persistent endpoint security and data risk management solutions for computers, laptops, tablets and smartphones, found the following:

- 15 percent of mobile workers believe they have little or no responsibility to protect the data stored on their personal devices
- 59 percent estimate the value of the corporate data on their phones to be less than $500
- About 33 percent of employees who had lost their phones did not change their habits afterward

To optimize productivity, employees spend time working both outside the office and behind their desks. In doing so, they want direct and convenient mobile access to sensitive corporate information. However, without appropriate training and security protocols in place, such access puts corporate confidential information at risk.

Corporations can employ the most sophisticated technical information security available, but as the large-scale data breaches over the last year have shown, not even the most sophisticated security can account for human error or complacency.

About the author. . .

*Elissa Doroff* (mailto:elissa.doroff@xlcatlin.com?subject=FFF%20article%20on%20mobile%20security)*, JD, is a vice president and product manager for XL Catlin's Cyber and Technology Underwriting team, where she works to minimize the frequency and severity of data breaches. With nearly a decade of cyber and technology insurance experience, Doroff often presents on these topics through panels and seminars for clients and industry associations and has published many industry-related articles.*

(/EditorPage.aspx?da=core&id=%7B8B3222A2-7D8E-4ADE-9361-8CD0B95DA994%7D&ed=FIELD53590736&vs&la=en&fld=%7B7D79FD1A-2A8F-474D-B514-D5FA7790F19B%7D&so=%252Fsitecore%252Fsystem%252FSettings%252FHtml#ednref1)Endnotes

1 FireEye, Out of Pocket: A Comprehensive Mobile Threat Assessment of 7 Million iOS and Android Apps, (Milpitas, Calif.: FireEye, February 2015), www2.fireeye.com/rs/fireye/images/rpt-mobile-threat-assessment.pdf (https://www2.fireeye.com/rs/fireye/images/rpt-mobile-threat-assessment.pdf) (accessed July 14, 2015).

2 Ponemon Institute LLC, The Security Impact of Mobile Device Use by Employees, December 2014, www.ponemon.org/library/the-security-impact-of-mobile-device-use-by-employees (http://www.ponemon.org/library/the-security-impact-of-mobile-device-use-by-employees) (accessed August 3, 2015).

3 Centrify Survey, Employees are Still Not Protecting their Mobile Devices (http://www.centrify.com/about-us/news/press-releases/2014/centrify-study-shows-employees-are-still-not-protecting-their-mobile-devices-

placing-organizations-at-risk/)
4Absolute Software 2015 U.S. Mobile Security Study (https://www.absolute.com/en/about/pressroom/press-releases/2015/absolute-survey-shows-millennials-represent-greatest-risk-to-corporate-data)