sierraware

Mobile Security Checklist

An Easy, Achievable Plan for Security and Compliance

Introduction

Are mobile devices the weak link in your security defenses?

Today, organizations are pouring millions of dollars into tools and services that can block malware and identify intrusions. And it's easy to see why; the number of data breaches is at an all-time high. In 2015, over 150 million records were reported compromised in 223 incidents.[1]

Unfortunately, while organizations lock down their network servers and PCs, they often don't enforce the same level of control on mobile devices, especially employee-owned phones and tablets.

However, with physical device theft accounting for over 15% of security incidents, organizations cannot ignore the threat that employees could leave their phones behind in airports and taxis and restaurants.

5.2 million
smartphones were lost or stolen in the U.S. in 2014[2]

74%
of organizations permit or plan to permit Bring Your Own Device (BYOD) at work[3]

Internet Exploits

Besides device loss and theft, mobility also increases the attack surface for threats such as snooping, man-in-the-middle, and brute force attacks by compelling organizations to make business apps accessible from the Internet rather than from an internal, protected network.

Insider Abuse

Mobile networking also allows malicious insiders to manipulate or steal data. While Data Loss Prevention (DLP) products might prevent users from saving confidential files to a USB drive or emailing them to a private account, these controls rarely extend to mobile phones and tablets. As a result, users can easily copy and paste confidential data into email or instant messaging apps or upload documents to file sharing apps.

Regulatory Compliance

Besides security concerns, organizations must comply with various IT security and privacy regulations. While every company must adhere to different standards, such as PCI DSS, NIST, FISMA, HIPAA, SOX, GLBA and more, several requirements are common across almost all regulations. These requirements including monitoring user access, correctly identifying end users with strong authentication, and encrypting data in transit. More specifically, organizations should record "who, what, when, and where" details for compliance audits.

If mobile users can view healthcare, financial, or other regulated data from their mobile devices, then IT must put in place sufficient safeguards to satisfy compliance.

"Telework and remote access technologies often need additional protection because their nature generally places them at higher exposure to external threats than technologies only accessed from inside the organization."

- NIST "Guide to Enterprise Telework, Remote Access, and BYOD Security"

[1] Privacy Rights Clearinghouse
[2] Consumer Reports
[3] Tech Pro Research Survey

Mobile Security Checklist

Addressing all of today's mobile security and compliance requirements might seem like an onerous task. But there are eight simple steps that IT can take that will reduce the risk of a data breach and address compliance.

1. Enforce Strong Authentication

To prevent unauthorized access and password guessing attacks, organizations should implement multi-factor authentication. The three main factors for authentication are something that a user knows, such as a password or PIN, something the user has, such as mobile device, or something the user is, such as a fingerprint.

Combining password-based authentication with a client certificate, device ID, or one-time password significantly reduces the risk of unauthorized access. Organizations can also implement time-of-day and location-based restrictions to prevent fraud.

> **"Account fraud and identity theft are frequently the result of single-factor authentication exploitation."**
>
> - FFIEC "Authentication in an Internet Banking Environment"

2. Encrypt Mobile Communications

With threats like snooping and man-in-the-middle attacks over Wi-Fi and cellular networks, IT should make sure that all communications between mobile apps and app servers are encrypted. Strong encryption that leverages 4096-bit SSL keys and session-based key exchanges can prevent even the most determined hackers from decrypting communications.

Besides encrypting traffic, IT should confirm that data at rest—the sensitive data stored on users phones—is also encrypted. For ultra-sensitive data, IT might want to prevent data from ever being downloaded to the end user device at all.

> **"Any sensitive information passing over the Internet, wireless networks, and other untrusted networks should have its confidentiality and integrity preserved through use of cryptography."**
>
> - NIST "Guide to Enterprise Telework, Remote Access, and BYOD Security"

3. Monitor User Activity

Maintaining a detailed audit trail is an essential way to identify insider abuse, accidental data leaks, and even malware-based attacks. Many compliance regulations mandate user monitoring to track access and changes to sensitive data.

If mobile users can view or edit confidential information such as healthcare, payment card, or customer data, then IT should monitor mobile user activity.

Log messages should identify when users access business apps and track users' geographic location and device ID. Failed login attempts and other errors should also be recorded.

For highly-sensitive apps, IT can record mobile user sessions to identify who did what and see the results from users' perspectives.

> **"Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise."**
>
> - PCI DSS Requirement 10: Track and monitor all access to network resources and cardholder data

Mobile screen recording delivers a complete picture of user activity.

4. Prevent Data Leaks

To avoid data leaks while still allowing users to install personal app on their mobile devices, IT must separate business apps from personal apps. Creating secure mobile workspaces helps prevent malware from accessing corporate apps and stop users from copying, saving, or distributing sensitive data.

For ironclad data leak prevention of confidential data:

- Control clipboard access to prevent copy and paste functions
- Block screen captures
- Prevent users from downloading confidential files to their phone or saving files on file sharing sites or connected devices or drives.
- Watermark sensitive files with users' usernames and timestamps

5. Protect Against Device Theft

Every year, millions of mobile devices are lost or stolen. To ensure sensitive data does not end up in the wrong hands, IT should provide a way to remotely wipe sensitive data or—better yet—make sure data is never stored on mobile devices in the first place.

For employee-owned devices, IT should lock or wipe corporate information while leaving personal apps and files intact.

When the device is found or replaced, IT should be able to quickly restore users' apps and data.

6. Patch App and Operating System Vulnerabilities

Recent Android and iOS vulnerabilities such as Stagefright and XcodeGhost have exposed mobile users to attack. In addition to mobile OS flaws, IT must contend with a never-ending succession of app updates and fixes.

To protect mobile users from attack, IT should check mobile devices and ensure that the latest patches and updates have been applied.

> **"More than 75 Percent of Mobile Applications will Fail Basic Security Tests Through 2015."**
>
> - Gartner Security and Risk Management Summit

7. Scan Mobile Apps for Malware

Eliminate malware and adware by testing apps for malicious behavior. Malware can be detected using virtual sandboxing or signature-based scanning tools.

For mobile workspace or virtual mobile solutions, perform malware scans at the server.

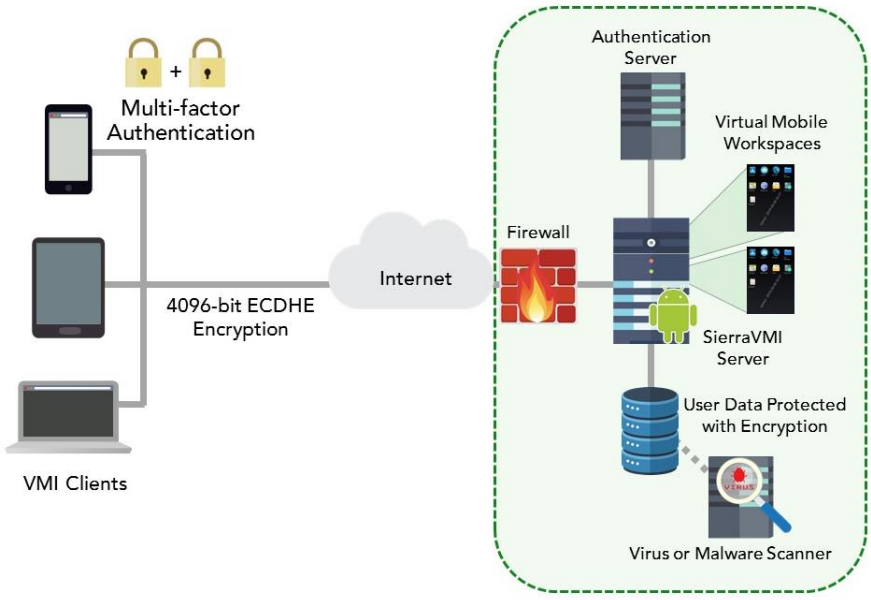
8. Train Employees

Educate employees about mobile security threats, such as social engineering and phishing attacks. Also inform employees of elevated risks caused by jailbroken and rooted phones and of sideloading apps from unsanctioned app stores.

Technologies that Help Address Mobile Security

Organizations may want to consider solutions such as Virtual Mobile Infrastructure (VMI) to secure their mobile apps and data. VMI allows organizations to host mobile apps on servers and provide remote access to these apps from any device. By virtualizing mobile apps, VMI enables businesses to:

- Avoid costly data breaches by preventing users from downloading sensitive data to their devices.
- Monitor privileged user activity with detailed logging and screen recording for forensics.
- Support heterogeneous environments with Android, Apple, and Microsoft devices.
- Block unauthorized access using multi-factor authentication based on a combination of passwords, certificates, device IDs and one-time passcodes.



A VMI deployment, with phones, tablets and laptops accessing a VMI server hosting mobile apps remotely.

With VMI, organizations host Android instances in their data center or in the cloud. Mobile users can then access Android applications remotely from iPhones, iPads, Android devices, HTML5-enabled Windows phones, and even Windows desktops.

"VMI delivers a secure virtual mobile device environment to a telework mobile device. Organizations considering the use of mobile devices for telework, particularly BYOD or third-party-controlled mobile devices, should investigate VMI technologies to see if they may be helpful in improving security."

- NIST "Guide to Enterprise Telework, Remote Access, and BYOD Security"

Conclusion

As organizations embrace BYOD, they need to develop a strategy to protect corporate data and satisfy compliance while supporting a broad array of mobile devices and apps. The mobile security checklist described in this paper documents the most important elements to any mobile security strategy. If organizations implement strong authentication, encryption, user monitoring, data leak prevention, and more, they will greatly reduce the risk of a data breach and satisfy most regulatory requirements.

Virtual Mobile Infrastructure, with its inherent ability to keep sensitive data off of devices and its robust security and auditing features, can help organizations quickly meet their mobile security and compliance goals.

About Sierraware

Sierraware is a leading provider of virtualization and security solutions that change the way applications are accessed and data is secured. Sierraware's virtual mobile infrastructure (VMI) software empowers developers to support all mobile platforms with a single app and to protect data and monitor user activity.

sierraware

1250 Oakmead Parkway
Suite 210
Sunnyvale, CA 94085
United States
Phone: +1 408-337-6400
Email: info@sierraware.com