GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

BYOD: Do You Know Where Your Backups Are Stored?

GIAC (GSEC) Gold Certification

Author: Marsha Miller, mmiller@mastersprogram.sans.edu
Advisor: Rick Wanner
Accepted: 30 June 2015

Abstract

Ever striving to reduce costs, companies in increasing numbers are testing Bring Your Own Device (BYOD) as a mobile solution. Although security has become a hot topic, ensuring the protection of confidential information during synchronization of a mobile device to a personal storage location may be overlooked. This paper will touch on elements of how and where data is stored on a mobile Apple and Android device, the default backup solutions, a few legal aspects to consider, and some security solutions offered by AirWatch and Good.

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

1. Introduction

With the availability of smartphones and tablets offered in today's market, companies are looking to capitalize on the mobile movement to improve productivity and availability of employees. In addition to the hefty price tag that can make it cost-prohibitive for a company to support a large number of devices, most employees prefer to carry a single device. In attempt to satisfy both sides, Bring Your Own Device (BYOD) has become increasingly popular. This solution allows the employees to use a personal device to access company assets, addressing both the employee's wishes and the company's financial bottom line.

This solution is not without its problems. When a company provides mobile assets to employees, it is easy to dictate the policies and procedures to cover every aspect of how both the data and device are handled. However with BYOD, a company should consider how to keep proprietary data secure and under control when it is on a personal asset. With the increase of breaches, the escalation of privacy concerns, and the desire to integrate the devices into enterprises more completely, mobile device security has come to the forefront.

Fortunately, there are some software options that can assist with mobile security and data control. And while information can be found relating to data in transit and data security on the device itself, backups are often left out of the equation. What happens to proprietary data during a backup?

1.1 BYOD and Backups

BYOD is an attractive solution for companies that want to save some money. If the employee is willing to use their personal device during business hours and for business use, the company does not have to purchase large quantities of devices to issue to employees. Not only does it save the company the cost of the device, but also there are fewer assets to track, fewer voice and data plans to purchase or maintain, and maybe even fewer software licenses to procure. Employees are happy because they get to use a familiar device and it is one less device to carry. They purchased a phone that had the exact features that they desire and not something they will be tempted to drop in the toilet when it aggravates them.

Marsha Miller, mmiller@mastersprogram.sans.edu Rick WannerRick Wanner

© 2015 The SANS Institute Author retains full rights.

Employees favor using personal devices for many reasons because they feel more connected with access to everything at their fingertips. However that connectedness may come at a price. They install applications and store information important to them just as a company does, often without regard to security. Aside from data stored on the device, if the company data is comingled with personal data, it may be inadvertently or intentionally stored in a backup located in the device owner's space and unreachable by the company.

2. Android vs iOS BYOD

Android and iOS have overtaken BlackBerry as the favored mobile device. Both platforms offer phone and tablet solutions providing a variety of choices for both personal and professional use. They share similarities as well as differences in the way they store data, both on the device as well as in the backup solutions.

2.1 iOS

A well-known innovator in mobile technology, Apple has progressed from its early roots in the client computing market to iconic music storage devices, phones, and tablets. iPod, iPhone, and iPad continue to be very popular devices and provide easy-to-manage backup solutions.

2.1.1 Data Stored on iOS

Apple mobile devices do not utilize external storage such as SD cards or USB drives, but instead only store data internally or on network resources such as iCloud. The iOS file system is based on UNIX and contains a similar structure. In general, applications are designed to be sandboxed and not interact with one another, although there are exceptions. To achieve this, the application is given a number of separate containers in which to store the data, and it is expected to operate solely within this environment.

In an Apple device, SQLite is used to store application data, which includes contacts, mail, text messages, call history, voicemail and the calendar. On the other hand, Property Lists, using XML or binary format, offer yet another way for applications to store and access data.

© 2015 The SANS Institute Author retains full rights.

They often contain information that allows a user to customize the application and allows tracking of information such as browser history or YouTube data (Hoog & Strzempka, 2011).

By default, a device does not store business data any differently than it stores personal data, which means that all data is lumped together, sharing the same space and subject to the same access permissions.

2.1.2 Local vs Cloud Backups

Backups in Apple products are created in one of two ways: by connecting the device to a PC or Mac (either wirelessly or via a USB interface cable) and using iTunes to synchronize, or synchronizing directly with iCloud. As Apple's initial backup solution, iTunes integrates with the mobile devices and provides a simple local backup solution. In Windows 7 and Windows Vista, it is stored in \Users*username*\AppData\Roaming\Apple Computer\MobileSync\Backup and in Mac OS X, it is ~/Library/Application Support/MobileSync/Backup (Hart-Davis, 2011). Although these are set by default, the location can be changed manually. Each time a backup is initiated, the file will be overwritten. A user has to manually copy the backup file to another location for preservation. Within iTunes, files can manually be selected for exclusion, and there is also a selection to enable encryption of the backups.

© 2015 SANS Institute, Author retains full rights.

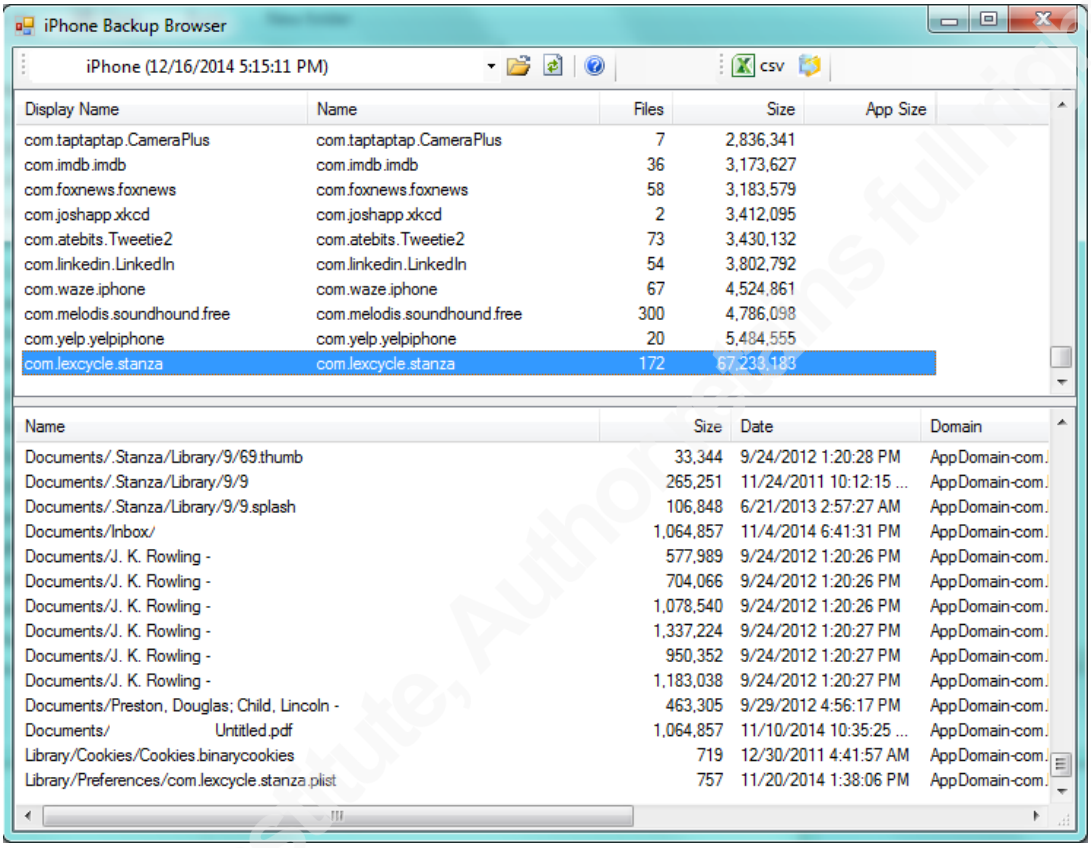
© 2015 The SANS Institute Author retains full rights.

Figure 2. iPhone 5 Sync. From "How to Do Everything iPhone 5" by Jason Rich, 2013, McGraw-Hill.

During a backup, most but not all of the information on the device is copied over to the backup location. This includes data unique to each device, such as preferences and application data. However it is not necessary to consistently duplicate static information that can be recovered in a factory restore operation, so synchronized data (such as mp3's, CD's and books) and the applications themselves are not included. This saves both space and time during the backup operation. Some items included in the backup are contacts, calendar events, call logs, photos, music, videos and SQLite databases for applications. Documents such as Word documents can also be transferred to and from a PC.

© 2015 The SANS Institute Author retains full rights.

When the directory is browsed, folders are stored in a tree below the iTunes folder which defaults to a user's profile directory. Some of the directories included in a backup are Application Support, Documents, Documents/Inbox and Library (Caches excepted).



One way for application developers to exclude files from backup is to use the key NSURLIsExcludedFromBackupKey ("Mac Developer Library: File System Details," 2015). The files contained in a backup have the extensions .plist, .mddata, and .mdinfo, and files with no extension. Carpene states, “Whilst these files exist with no extension, it can be difficult at a glance to determine what the file actually is. These files are, in fact, a number of different files and formats, including images, videos, voice recordings, sqlite databases, text documents, and other miscellaneous files, with their extension removed. The extension-less files contain all of the actual documents and files that have been backed up from the suspect phone” (Carpene, 2011).

Marsha Miller, mmiller@mastersprogram.sans.edu Rick WannerRick Wanner

© 2015 The SANS Institute Author retains full rights.

Although local backups via iTunes were initially the only backup solution offered by Apple, iCloud is now included as an option. An attractive feature for users, it provides quick access to data recovery as well as additional storage and a central location from which to share data across multiple devices. Applications create the same files and directories whether they are stored locally or in iCloud ("Mac Developer Library: File System Details," 2015). However items that are already synchronized with iCloud such as e-mail, contacts, and calendars are not included in the backup. It is important to note that iCloud is fully integrated with the Apple mobile devices by default, but other solutions, such as Dropbox, can also be used.

Also of note, encryption is not enabled by default on backups. So when an employee plugs a mobile device into a personally-owned computer or synchronizes with personal storage in the cloud, there is nothing to restrict company data from inclusion in a personal backup, and it may be unprotected from prying eyes with a dedicated purpose. That could be very bad news if the company has data it does not want to share.

Apple devices, such as iPad and the more recent versions of iPhone, provide encryption, both in transmission and hardware for the device. However, encrypted backups are still not bulletproof. Hoog and Strzempka state, "In particular, the data contents within encrypted backup files can be unencrypted and viewed with the use of inexpensive software" (Hoog and Strzempka, 2011). As stated on Apple's website, data stored in the iCloud is transmitted using AES-128 bit encryption during transit as well as while it is stored; however, AES-256 bit encryption is used for passwords and credit cards for both storage and transmission.

Although Apple has additional Mac software and features that work with third-party software to allow the configuration of a device for security purposes, business and personal data are typically comingled in the same space. Without utilizing any of the security features, data is essentially unprotected and can easily be included in a backup outside of the company's control.

2.2 Android

Although Android devices were not first on the market, they have grown in popularity over the years. As an open-source platform, multiple manufacturers offer a tantalizing array of

© 2015 The SANS Institute Author retains full rights.

sizes and features that are an attractive option to the "one-size-fits-all", closed-source Apple devices.

2.2.1 Data Stored on Android

The Android kernel is based on Linux and uses EXT (Extended File System) for the operating system, although YAFFS was previously de facto. A separate subdirectory is created for each application when it is installed on an Android device. It often takes the form of /data/data/<application name> and stores the application files, shared preferences, and databases. Email messages, contacts, calendar, and other important information are stored in the separate applications.

Android uses SQLite databases to store application data in a retrievable fashion. Because it contains information such as contacts, text messages and call history in single cross-platform file, the database is easy to capture in a backup. In addition, shared preferences contain additional data stored as an XML file.

2.2.2 External Storage

Although Apple unwaveringly sticks to internal storage only, many Android devices allow for the use of external storage. An SD card can be inserted or a USB device can also be connected with the use of an additional cable. While the internal storage uses strict guidelines to dictate the structure of how and where data is stored, data on SD cards, utilizing the FAT32 formatting, is less rigid. Data here is stored in a typical tree structure similar to Linux, but security cannot enforce permissions in a similar fashion as with internal storage (Hoog, 2011). This means that any data stored in external storage is not secure by native means.

2.2.3 Local vs Cloud Backups

Unlike the software interface offered by Apple's iTunes product, Android's local backup solutions to the PC and Mac are a little different. Some Android manufacturers provide a method of backup via USB to PC. For instance, Samsung provides an application that can be installed called Kies ("What can I backup and recover from my device using Kies? : Cell Phones | Samsung," 2014). HTC provides offers HTC Sync Manager as an option ("HTC One – About HTC Sync Manager – SETTINGS & SERVICES – How-tos – Support | HTC Singapore," n.d.).

© 2015 The SANS Institute Author retains full rights.

Of course, some people may prefer more granular control of their data instead of relying on automation and an additional piece of software installed on the PC. By connecting the device via USB to the PC, one can simply navigate through the directory and copy the data from one device to the other. When a mobile device is connected to a Windows 7 PC via a USB cable, Windows identifies the device, loads the proper drivers, and assigns the new device a drive letter. At this point, the device can be viewed in Windows Explorer and files can be transferred between the devices. If an SD card is also present in the device, the internal storage and the SD card are presented separately.

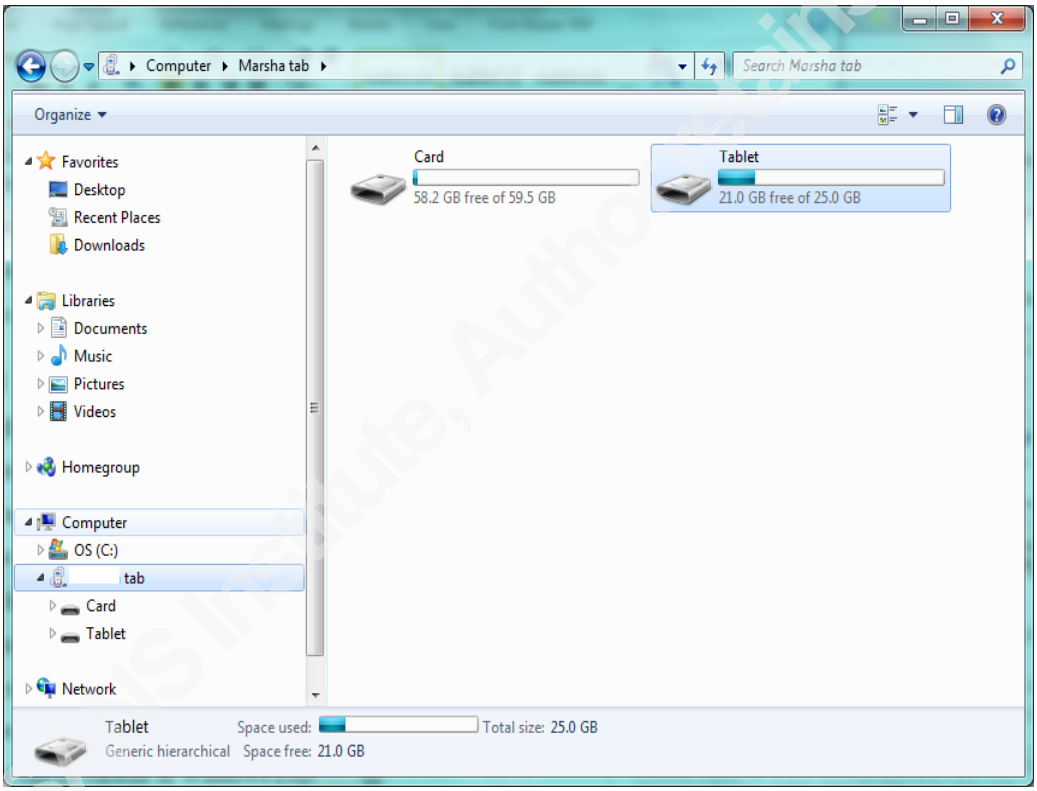


Figure 1. Android Sync

There are additional options for more traditional backup operations that are not native to the system, and applications in the Google Play Store that can be downloaded. Another option more suited to a power user is the adb backup command used from a shell, which will also create an encrypted backup if the device itself is encrypted.

Marsha Miller, mmiller@mastersprogram.sans.edu Rick WannerRick Wanner

© 2015 The SANS Institute Author retains full rights.

In addition to applications, documents, and other data, backups can also be stored on an SD card. Applications such as Super Backup, MyBackup Pro and Helium create a backup of messages, calendars, contacts, and more.

Depending on the manufacturer, options for cloud backups include Box, Dropbox, Google Drive, Spider Oak, and Microsoft's OneDrive; however most Android devices default to the Google Drive solution. As a manufacturer specific solution, HTC Backup stores contacts, text messages and even login credentials for email and social network accounts on Google Drive or Dropbox ("HTC One – Using HTC Backup – SETTINGS & SERVICES – How-tos – Support | HTC Singapore," n.d.).

In the case of Drive and similar to Apple, only contacts, phone settings and applications are backed up. Unlike Box or Dropbox which also encrypt data at-rest using 256-bit AES, Google Drive only encrypts data in transit using SSL.

Although application developers have the option to control whether or not the data from their application is included in a backup by setting an attribute in the AndroidManifest.xml file, it does not provide a clear delineation between business and personal data. Also, because this solution relies on each individual application developer for configuration, it not a reliable solution for either device or data owners that need the flexibility to set exact restrictions according to their needs.

3. Protecting Data

One simple method to protect a backup is to encrypt it prior to storing it locally or in the cloud. However, this protects the backup in whole and does not address segregating company information from private. Several methods have been created to protect proprietary information on mobile devices, and some even address the issue of backups. Mobile Device Management (MDM), Mobile Application Management (MAM) and Mobile Content Management (MCM) are a few examples. Despite the descriptive titles, these concepts are often confused and used interchangeably. In fact, each has a unique framework with pros and cons. Not only that, whether or not a device is capable of device encryption will also affect the usefulness of some tools.

© 2015 The SANS Institute Author retains full rights.

3.1 MDM, MAM, and MCM

The concept behind Mobile Device Management is to provide security for the device as a whole. It is achieved by monitoring, configuring, and securing the device to allow a company to control the use and the restrict the data access. Some aspects of the configuration work in a similar fashion to that of Group Policy used in a Windows environment. In other words , it has settings that turn on and off features of the mobile device, such as allowing access to the browser, restricting the employee from changing the wallpaper, or requiring a passcode to unlock the device. One feature included in Apple products to support MDM is the ability to restrict iTunes and iCloud backups.

Mobile Application Management, on the other hand, secures specific applications that the company distributes instead of configuring the entire device. A company can develop its own applications with security built in or it can "wrap" third-party applications with additional code to apply security. This allows employees to access company data in a structured way without impacting the general use of the device. This works well for personally owned devices and as an extension to business partners. However, the company may need to employ application developers to support this implementation. Also, in cases where the company does not own the asset, it may be difficult to provide support due to the lack of device standardization. The application may function well on an iPhone, but fail to perform optimally on an Android device or on an older version of iPhone.

Mobile Content Management allows a company to share documents with employees, partners, contractors and others. It operates as a separate container installed on the device which uses authentication and authorization to control access to data repositories providing a secure collaboration area. It is different from MAM in that it creates one single container as opposed to multiple applications with different functions. The container may be restricted to read-only or may allow editing, according to the configuration settings made by the administrator. And in the same way that MAM allows more freedom of the device settings, so does MCM.

But what happens to the company data if the user initiates a backup? The good news is that with proper use of tools such as these, proprietary business information should not be at risk. Personal backups should never contain any proprietary data. Regardless of the solution chosen, it

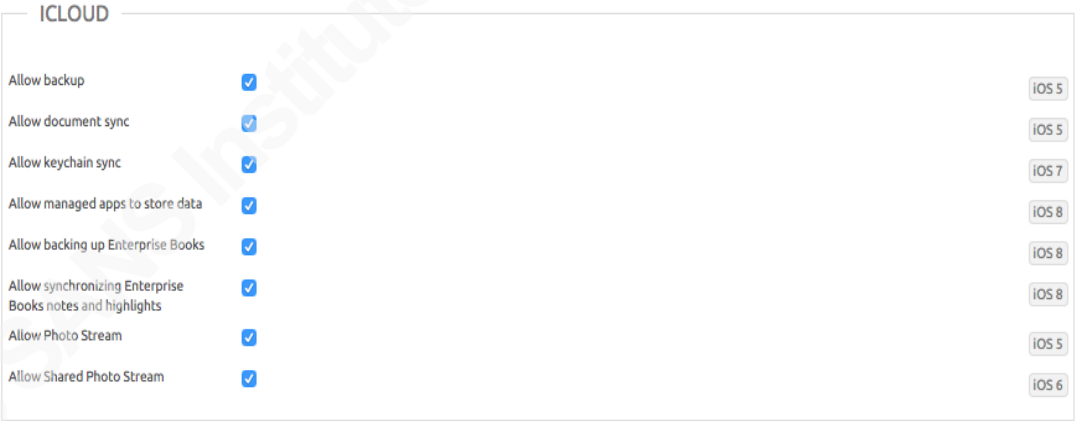
© 2015 The SANS Institute Author retains full rights.

is important to inquire with the software provider in regards to the impact on personal backups and data synchronization. The right choice provides a secure solution that protects the integrity of both company and personal data recovery without compromising security.

3.2 AirWatch

AirWatch offers several products that cover MDM, MAM, and MCM. The suites use a system of profiles installed on devices that can be configured for granular control. In addition, AirWatch includes file distribution over an encrypted connection. Secure Content Locker (which provides access to repositories such as SharePoint or file server directories) states that it utilizes AES 256-bit encryption for in-transit, in use, and at-rest (AirWatch, 2015).

AirWatch uses both native features and OEM-specific API integration to enact security settings in MDM. Available through AirWatch Software Development Kit (SDK) and suite of applications, companies can apply a combination of MDM API's and Data Loss Prevention (DLP) policies to prevent proprietary data from being included in a personal backup file, however the exact method may differ depending on the device (C. Clack, personal communication, May 27, 2015).



One feature offered by AirWatch allows both the internal drive as well as any removable drives to also be encrypted for capable devices, while providing a separate solution for those that are not. The company also has a solution that covers the use of third-party cloud storage (AirWatch, 2015). While MDM would typically present a challenge that may result in an

© 2015 The SANS Institute Author retains full rights.

employee's personal data being wiped during a device wipe, AirWatch has an enterprise setting to protect against this.

3.3 Good

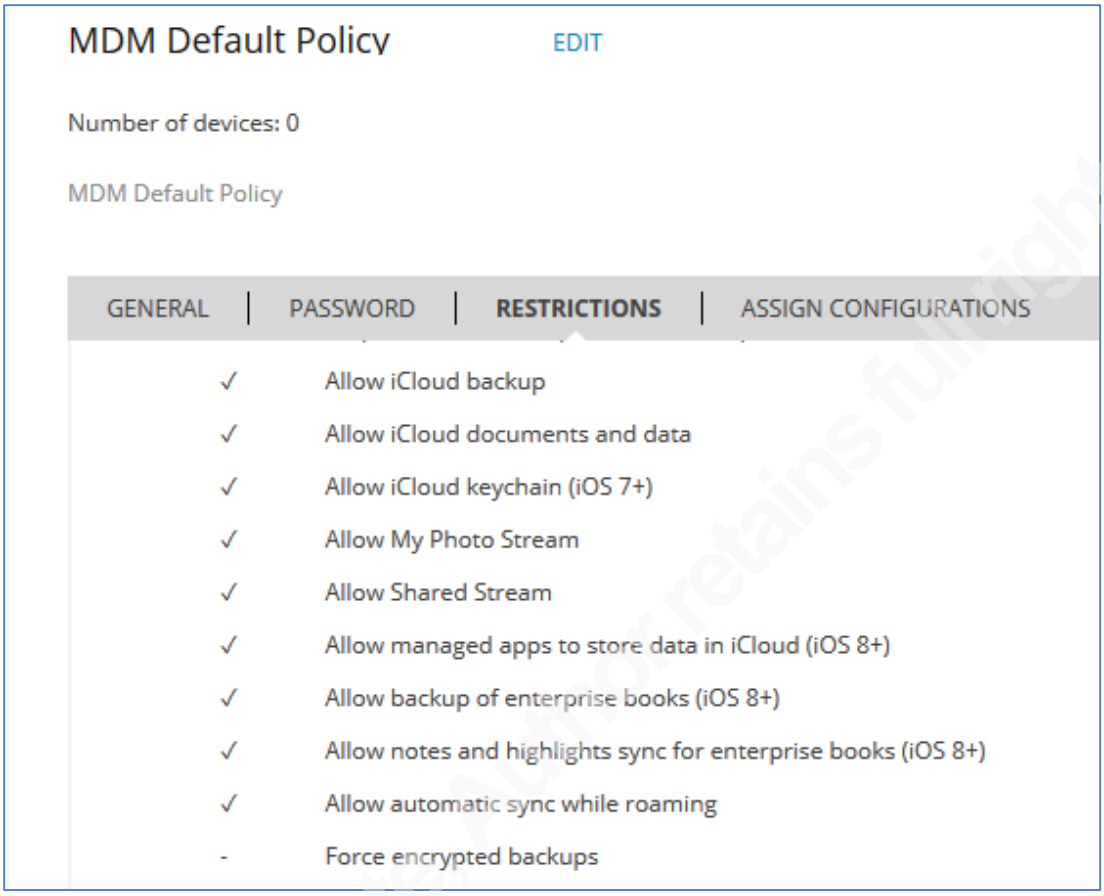
Good Technology is another company that offers data protection services in a variety of selections. Similar to AirWatch, has a selection of suites that cover MDM, MAM, and MCM. While MDM is provided in all suites, it is not a required implementation.

In the environment, the Good client database stores all of the enterprise data, including email and calendar appointments, in an encrypted state. The documentation states the method of encryption takes the client's password "concatenated with a random 64-bit salt generated using a random number function." (Security and architecture. A technical whitepaper, 2014) Also the data at-rest in the Good containers is protected by AES encryption however the specific level is not listed.

Although the documentation does not mention whether or not the Good client database is included in a backup to a personal storage solution or if it can be copied to another device via USB or wireless, Good does state that backups do not include information stored in the MAM-style containers provided by Good Dynamics (Good Technology, 2014). One interesting selection offered on part of MDM can control whether or not an iOS device is allowed to create an iCloud backup. It can also enforce backups to be encrypted.

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.



In addition to iOS settings, Good has a few Android settings as well. KNOX is used extensively with Samsung products to provide additional control, but none appear to specifically address backups.

4. Lost Data Management

Segregating and encrypting files prior to a backup is a good start, but preventing the data of concern from inclusion in a backup is ideal. If implemented properly, MDM can restrict backups on some devices, and the data should be encrypted with the use of MAM and MCM, even if it is included in a personal backup solution.

As a matter of policy, an agreement between the company and the employee is highly recommended, and should be signed by the employee granting consent. According to Benjamin Wright, it is important to inform and remind employees about the risks involved in a BYOD

© 2015 The SANS Institute Author retains full rights.

situation. He adds that laws are open to interpretation, but assets, both mobile devices as well as PC's, can be seized during litigation. He outlines the agreement should include the company's policy and the procedures that will be enacted during a breach. It should also address employee privacy and damage to the device (Wright, n.d.).

However, it is important to have a plan in place to address the possible loss of data and every aspect should be considered. Was the data copied to a personal computer at an employee's house via a backup? If so, does the company have any way of recovering the data or wiping the device? A data protection plan will establish guidelines to prevent spills as well as the steps to take when one occurs (NSA, 2012).

This issue is especially important to consider when the information involved is governed by the Department of Defense or addressed by specific laws, such as Personally Identifiable Information (PII). DLP is identified in the SANS Twenty Critical Security Controls and should be implemented to monitor and identify loss of proprietary information ("Critical Security Controls," n.d.).

4.1 Legal Aspects of Data Recovery

Data recovery can be tricky so it is important to engage legal counsel as soon as data loss is detected. An important question in whether or not a company has any right to an individual's private backup revolves around who owns the data. According to Castle (Castle, 2014), personal data may be used in a legal action if it is pertinent to an organization's litigation (Castle, 2014). If there are multiple backups involved, all backup files will need to be recovered. Other potential issues could involve theft of or improper disposal of personal storage drives and SD cards containing backup files.

4.2 Other Legal Implications

Although some solutions mentioned such as MCM allow for segregated containers of business data to be deleted without harming the personal data, other solutions may not. One legal issue presented is whether or not monitoring software, such as MDM, is appropriate on personal devices even in cases where the individual has agreed (Grover, 2013). While employees may have signed legal agreements, third-parties, outside partners and customers may not be covered

© 2015 The SANS Institute Author retains full rights.

in such a manner. Also, if the encrypted information is copied onto another device, are there legal implications for just possessing the file even if it is not world-readable?

The responsibility to protect information does not stop with active data. It includes all data including that which is contained in a backup. Not only should a company protect its data for proprietary reasons, they are legally responsible to protect certain types of information.

Depending on the data involved on the devices, different government regulations and laws may come into effect. One federal law in particular of note is the Computer Fraud and Abuse Act (CFAA). The CFAA is intended to address the unauthorized access of a computer. This includes both intentionally accessing it without authorization or exceeding the scope of approved access.

Other federal laws that may affect digital data are the Electronic Communications Privacy Act (ECPA), the Digital Management Copyright Act (DMCA), Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act of 2002 (FISMA), and Sarbanes-Oxley Act (SOX). Many states also have laws that govern the inadvertent public disclosure of information requiring companies to notify those affected when personally identifiable information (PII) is released without permission.

The bottom line is that due diligence is a good idea when considering the legal implications of BYOD. Always involve the company legal department when considering changes in policy. Consider both the impact of company information contained in personal backup solutions as well as personal data contained in corporate backup solutions.

5. Conclusion

BYOD may be a suitable solution for some companies, allowing employees access to company resources using personal mobile devices. But with the benefits, there are some risks to consider. Other than the financial ramifications involved in the loss of data, there are potentially legal ones as well. In the overall scheme, any connections that can be made to the device,

© 2015 The SANS Institute Author retains full rights.

including synchronization with backup solutions, are a concern that should be carefully addressed.

Some software solutions that can assist in data management are MDM, MAM, and MCM. In addition, a legal agreement between the company and the employee is helpful in clearly defining policy and procedures, and the company should have a security plan that outlines steps to be taken during a breach.

By understanding the company's environment, the direction of its objectives, and how it would like to use its assets, a multi-layered solution can be put in place to protect its most important asset: its data. While there are many ways to protect data, the impact of personal backup solutions should not be overlooked.

Marsha Miller, mmiller@mastersprogram.sans.edu Rick WannerRick Wanner

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

References

Don't believe the hype - all containers are not equal. protecting the 3 Cs of secure mobility. (2014). Retrieved from Good Technology website: https://www1.good.com/resources#whitepapers

Carpene, Clinton. (2011). Looking to iPhone backup files for evidence extraction. In Secau Security Congress & Edith Cowan University (Eds.), *Building a resilient future: 2011 secau Security Congress : proceedings of the 2011 secau Security Congress, Perth, Western Australia, 5-7 December 2011*. Retrieved from http://ro.ecu.edu.au/adf/92

Castle, L. (2014, October 20). Who Owns BYO Data? *Mobile Enterprise*. Retrieved from http://mobileenterprise.edgl.com/news/Who-Owns-BYO-Data--95967

Grover, Justin N. (2013). *Android forensics: Automated data collection and reporting from a mobile device* (10). Retrieved from Science Direct website: http://www.sciencedirect.com/science/article/pii/S1742287613000480#articles

Hart-Davis, G. (2011). *IPad & iPhone administrators guide: Enterprise deployment strategies and security solutions*. Retrieved from http://www.books24x7.com

Hoffman, C. (2013, March 14). HTG Explains: What Android Data is Backed Up Automatically? Retrieved from http://www.howtogeek.com/140376/htg-explains-what-android-data-is-backed-up-automatically/?PageSpeed=noscript

Hoog, A. (2011). *Android forensics: Investigation, analysis, and mobile security for Google Android*. Retrieved from http://www.books24x7.com

Hoog, A., & Strzempka, K. (2011). *IPhone and iOS forensics: Investigation, analysis, and mobile security for Apple iPhone, iPad, and iOS devices*. Retrieved from http://www.books24x7.com

HTC One - About HTC Sync Manager - SETTINGS & SERVICES - How-tos - Support | HTC Singapore. (n.d.). Retrieved March 23, 2015, from http://www.htc.com/sea/support/htc-one/howto/333189.html

HTC One - Using HTC Backup - SETTINGS & SERVICES - How-tos - Support | HTC Singapore. (n.d.). Retrieved March 23, 2015, from http://www.htc.com/sea/support/htc-one/howto/333185.html

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

iCloud: iCloud storage and backup overview. (2015, February 3). Retrieved March 23, 2015, from https://support.apple.com/kb/PH12519?viewlocale=en_US&locale=en_US

Mac Developer Library: File System Details. (2015, March 9). Retrieved March 27, 2015, from https://developer.apple.com/library/mac/documentation/FileManagement/Conceptual/FileSystemProgrammingGuide/FileSystemDetails/FileSystemDetails.html#//apple_ref/doc/uid/TP40010672-CH8-SW

Mavretich, R. (2012). Legal Issues within Corporate "Bring Your Own Device" Programs. *SANS Reading Room*. Retrieved from http://www.sans.org/reading-room/whitepapers/legal/legal-issues-corporate-bring-device-programs-34060

Mobile content management. (2015). Retrieved from AirWatch by VMware website: http://www.air-watch.com/resources/white-papers/

Mobile content management: Top 10 considerations. (2015). Retrieved from AirWatch by VMware website: http://www.air-watch.com/resources/white-papers/

NSA. (2012). *Securing Data and Handling Spillage Events*. Retrieved from https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/fact_sheets.shtml

Protecting criminal justice information: Achieving CJIS compliance on mobile devices. (2015). Retrieved from AirWatch by VMware website: http://www.air-watch.com/resources/white-papers/

Rich, J. (2013). *How to Do Everything iPhone 5*. Retrieved from http://www.books24x7.com

SANS. (n.d.). Critical Security Controls. Retrieved May 4, 2015, from https://www.sans.org/critical-security-controls/

Security and architecture. A technical whitepaper. (2014). Retrieved from Good Technology website: https://www1.good.com/resources#whitepapers

What can I backup and recover from my device using Kies? : Cell Phones | Samsung. (2014, April 21). Retrieved March 23, 2015, from http://www.samsung.com/us/support/SupportOwnersFAQPopup.do?faq_id=FAQ00029017&fm_seq=29185

Wright, B. (2012, March). Bring Your Own Device Policy - Part 1 | InfoSec DFIR Law [Web log post]. Retrieved from http://hack-igations.blogspot.com/2012/03/byod-policy.html

Marsha Miller, mmiller@mastersprogram.sans.edu Rick WannerRick Wanner

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

Wright, B. (n.d.). *Bring Your Own Stuff: Law*, *Policy & Investigations* [Power Point slides].

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

Last Updated: March 29th, 2017

Upcoming Training

Click Here to {Get CERTIFIED!}

Mentor Session - SEC401	Hollywood, CA	Apr 07, 2017 - May 05, 2017	Mentor
Mentor Session AW - SEC401	Grand Rapids, MI	Apr 07, 2017 - May 19, 2017	Mentor
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201704,	Apr 11, 2017 - May 18, 2017	vLive
Community SANS Cleveland SEC401	Cleveland, OH	Apr 17, 2017 - Apr 22, 2017	Community SANS
SANS Baltimore Spring 2017	Baltimore, MD	Apr 24, 2017 - Apr 29, 2017	Live Event
Community SANS Virginia Beach SEC401*	Virginia Beach, VA	Apr 24, 2017 - Apr 29, 2017	Community SANS
Mentor Session - SEC401	Edmonton, AB	Apr 26, 2017 - Jun 07, 2017	Mentor
SANS Riyadh 2017	Riyadh, Saudi Arabia	May 06, 2017 - May 11, 2017	Live Event
Community SANS Las Vegas SEC401	Las Vegas, NV	May 08, 2017 - May 13, 2017	Community SANS
SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
Community SANS Columbia SEC401	Columbia, MD	May 15, 2017 - May 20, 2017	Community SANS
Community SANS Baton Rouge SEC401	Baton Rouge, LA	May 15, 2017 - May 20, 2017	Community SANS
SANS Northern Virginia - Reston 2017	Reston, VA	May 21, 2017 - May 26, 2017	Live Event
SANS Melbourne 2017	Melbourne, Australia	May 22, 2017 - May 27, 2017	Live Event
SANS London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Atlanta 2017	Atlanta, GA	May 30, 2017 - Jun 04, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event