Abstract

The phenomenon of Bring Your Own Device (BYOD) is one of the new issues that each security professional will have to address in their security planning. The security professional will have to take into consideration how much, if any, BYOD access will be allowed and how to handle issues that will arise from the use of someone’s personal device(s) on the corporate network. This research seeks to identify the problems, find the usage policies and, device security software related solutions that can assist each security professional in controlling this daunting security issue.
Table of Contents

Abstract .............................................................................................................................................. 2
CARE AND CONTROL OF INFORMATION IN THE BYOD ERA ......................................................... 4
Chapter 1: Introduction ...................................................................................................................... 4
Thesis Statement ............................................................................................................................ 5
Chapter 2: Review of Literature ......................................................................................................... 6
  How does the IT department control the BYOD environment? ..................................................... 6
  What about terminated, laid off, or resigned employees? ............................................................ 7
  Lessons Learned ............................................................................................................................. 8
Chapter 3: Research Methodology .................................................................................................. 10
Chapter 4: Results ............................................................................................................................ 11
Chapter 5: Conclusion and Recommendations ................................................................................ 12
  Company Considerations .............................................................................................................. 12
  User Considerations ..................................................................................................................... 12
References ........................................................................................................................................ 14
Appendix A – Major Retailer Security Policy Examples ................................................................. 15
  Remote Access Policy ................................................................................................................... 15
  Mobile Security Policy ................................................................................................................ 17
  Mobile Media Standard ............................................................................................................... 20
Chapter 1: Introduction

When we first began using computers to keep track of and manipulate data it was the size of the equipment that provided a major part of the security. The fact that you had security systems controlling access not only to the buildings but the computer room itself made security easier. The only method to sneak out the data would have been to carry out a report and the security guard usually was on the watch for such activity.

Then we moved up to the ability to have a computer in our own homes that allowed us access to corporate information assets. This brought on a whole new set of security issues. There have been many strides made in controlling this type of information by using virus scanning and monitoring programs. It made security more relevant for Information Technology (IT) and it made it necessary for corporations to create a specific department to control this problem.

Jump ahead thirty years and now most employees have computers, smart phones, laptop computers, and tablet computers. This has made it so much harder to control and each company must consider these devices in their security planning. Does the company want to allow BYOD usage? What policies will be necessary to control the security of corporate information? Will the company assist the employees in the cost of their personal devices?

BYOD is the newest problem facing the IT security departments and this report will examine these issues and determine if there are solutions for the problems. It is something that most companies are just beginning to address and it is probably the most dangerous threat to information security in current times.
**Thesis Statement**

BYOD is the newest security issue facing corporate security professionals and there are many things to be considered before allowing this new trend into the corporate network arena. This should bring with it a heightened sense of security regarding BYOD policies and the use of necessary tools that could allow employees increased productivity and communication without giving up the security necessary for any company.
Chapter 2: Review of Literature

How does the IT department control the BYOD environment?

The number one thing for securing BYOD is to make sure that you use some sort of Mobile Device Management (MDM) software to allow the IT staff to track and control the BYOD devices being utilized on the corporate network (Ullman, 2013).

There are many to look at here are just a few:

- **Notes Tracker from IBM** ("Social Business Anytime, 2013)
  - Allows access to your Lotus Notes from your mobile device
  - Allows access to business systems and information
  - Allows Security Professional to wipe the phone remotely if necessary
    - Drawback here, it means all of the phone will be wiped clean including personal information on the device

- **MaaS360** (Maas360, n.d.)
  - Provides for the possibility of backup and restore services
  - Strong Encryption of Data
  - Allows for Security Professional to establish and enforce compliance to company policies
o  McAfee Enterprise Mobility Management  ("McAfee Announces new Enterprise.",2012)

  •  Blocks cloud backup
  •  Stops malware from entering the company system
  •  Low power usage
  •  Will soon expand to include Android and smartphones

These are just a few of the major players on the market and new software is being released on a regular basis.

What about terminated, laid off, or resigned employees?

The idea of using BYOD seems like a great solution to the company but there could be unexpected reasons this great idea can go bad. Like all security, people are the weakest link in BYOD so you need to plan for the employee issues that arise on a regular basis (Schmeiser, 2013). The trick is to strike a balance between the BYOD of workforce with the risk of company assets exiting the building when a company takes action against an employee (Schmeiser, 2013).

What would happen in the case of a layoff? Right now we all know that all of employees take some sort of corporate data when they leave, on good or bad terms. Policies will need to be put in place to handle this problem which grows larger when you add in BYOD access termination (Schmeiser, 2013).
Lessons Learned

Indoff Incorporated’s Director of IT Systems, Shawn Faulkingham offers these guidelines if you are considering allowing BYOD into your corporation (Ullman, 2013):

- Build your application that will work on any device
- Test everything thoroughly prior to deployment.
  - This would have to include any security and access issues that could represent a threat to the corporation’s data
- Remember there will be new devices that you will have to accommodate on a constant basis.
  - Each new device, application, or operating system represents a new risk to your security plan
- Money Crashers Personal Finance’s Gyuate Park, co-owners of this small company began using BYOD for his 35 employees about a year ago (Ullman, 2013):
  - Make sure you have a complete BYOD policy prior to allowing BYOD usage
  - Have security policy in place that includes
    - What is acceptable use?
    - How organizational data will be handled should an employee leave the company
  - Require password protection of the device
  - Allow for a remote wipe of the BYOD
A survey performed by Dell Quest Software taken from 1,500 IT executives regarding BYOD and found the following (Ullman, 2013):

- 75% of the organizations who implemented a BYOD program reported an increase in the employee productivity, response times to customers, and better work processes.
- 70% of these organizations said it improved collaborations among teams.
Chapter 3: Research Methodology

I was fortunate to get access to an interview with a major retailer in the central area of Michigan. On October 16, 2013 I was provided thirty minutes of time to discuss the topic of BYOD in the workplace at his place of employment. The following is an account of our discussion.

I found this security professional open to assisting me and helping fill in some of the blanks when it comes to the actual use of BYOD in his workplace. The only request that was made was that I keep the company and his identity confidential, I have respected that in this document.

We discussed what usage of BYOD is allowed at his company. They allow only the access to the Lotus Notes functionality on BYOD devices. They control this access with IBM’s Notes Tracker Software. Each user is required to have their devices configured by the security department according to the policies that are in the appendix and get sign off from the user that they understand the expectations of both sides of the agreement. This does contain the one problem many of the personal users dislike; If necessary the security department can wipe all data from the BYOD, personal and professional. Most of their users did not object to this drawback (Security Professional, personal communication, 10/16/2013).

In the future this major retailer would like to make BYOD more robust access to the company data assets. This is in the planning phase and part of this research is the correct software to meet the MDM needs (Security Professional, personal communication, 10/16/2013).
Chapter 4: Results

This research supports that BYOD is not just a trend but, the new reality that must be dealt with by company security professionals. It seems to be growing slowly enough that this may represent one of the first technologies where security can be a forethought instead of an afterthought. BYOD is here to stay.

The biggest weakness identified was that few companies addressed the need for continuous training of their user community in security issues. It is important that you include these users because it has been proven over and over that people represent the company's biggest risk to security. It is essential that each company have continually updated security policies and plan for the continuous education of their users.
Chapter 5: Conclusion and Recommendations

Company Considerations

The biggest conclusion from this research has been the need for security education on the user level. BYOD is not going away based on the usage percentages found in literature research. The company must have strong security policies, strong MDM software to control the access, and full cooperation from their staff in following the policies.

There is an old saying; “Trust but Verify.” This is why the security software is in a constant state of flux and will remain this way for the foreseeable future. This means that you may be asked to turn your device over to the company IT department for updates and new software to be installed.

When companies look to the future they must be willing to consider the use of BYOD by their employees as an asset they must control.

User Considerations

When you consider the idea of using your own device for personal and business you must accept the idea that you will be allowing your employer access to all of your personal information stored on your device. You are faced with the reality that even though it is your device once you are allowed to use it for work it does become a company asset as well (Kendrick, 2013).

Your employer will install software and may even place it in a separate area from your personal data but at any time the employer decides they need to audit your device or make upgrades they will also have access to the personal information, photos, website history and any other application you have loaded to your device. You will be asked to sign an agreement that allows this or you will more than likely not be able to use the device for work (Kendrick, 2013).

The only way to avoid this issue is to keep your personal data off the device. That in effect defeats the purpose of using your personal devices to reduce the number of devices you must carry or maintain.
If you avoid using the device for personal information then you may as well accept the company equipment and use your own equipment for personal purposes only. While it may be cumbersome to carry two phones it may be more embarrassing to have your employer find personal information on your device during an audit that may actually result in your termination (Kendrick, 2013).

“It is important to realize that even though you own the phone and you keep the non-work stuff separate from the work activities, that information is still exposed to the employer upon demand. If the company IT people need to see your phone, it’s out of your hands (literally) and there’s nothing you can do about it. At that point it’s only sort of your phone (Kendrick, 2013).”

Much thought should be put into your decision to use your personal devices for work.

- Do you want your employer reading your e-mails, texts, personal documents stored on the device?
- Do you want your employer to view all of the pictures you have stored on your device?
- What if the music you have on your device does not fall in line with the company philosophy?
  - Example: You work for a religious organization and you prefer to listen to rock or rap music that contains lyrics that might be perceived as offensive to your employer
References


1.0 Overview

Remote access methods and tools, provide a way for computer users and support staff alike to share screens, access work computer systems from home, and vice versa. Examples of such software include Cisco’s IPSEC and Any Connect VPN. Examples of methods include Direct Access from Internet To Major Retailer, Direct Access via VPN from Internet To Major Retailer, Access for BYOD. While these methods and tools can save significant time and money by eliminating travel and enabling collaboration, they also provide a back door into the Major Retailer network that can be used for theft of, unauthorized access to, or destruction of assets. As a result, only approved, monitored, and properly controlled remote access tools may be used on Major Retailer’s computer systems.

2.0 Purpose

This policy defines the requirements for remote access tools used at Major Retailer.

3.0 Scope

This policy applies to all remote access where either end of the communication terminates at a Major Retailer computer asset.

4.0 Policy

All remote access methods and tools used to communicate between Major Retailer’s assets and other systems must comply with the following policy requirements.

4.1 Remote Access Methods and Tools

1. The company provides mechanisms to collaborate between internal users, with external partners, and from non-Major Retailer systems. The approved methods and software list can be obtained from Information Technology Security Group. Because proper configuration is important for secure use of these methods and tools, mandatory configuration procedures are provided for each of the approved tools. See Major Retailer Remote Access Standards.

2. The approved methods and software list may change at any time, but the following requirements will be used for selecting approved products:
   a) All remote access tools or systems that allow communication to Major Retailer resources from the Internet or external partner systems must follow Major Retailer Remote Access Standards.
   b) The remote access tools authentication database source must be Active Directory or LDAP, and the authentication protocol must involve a challenge-response protocol that is not susceptible to replay attacks. The remote access tool must mutually authenticate both ends of the session.
   c) Remote access tools must support strong, end-to-end encryption of the remote access communication channels as specified in the Major Retailer network encryption protocols policy.
   d) All Major Retailer anti-virus, data loss prevention, and other security systems must not be disabled, interfered with, or circumvented in any way.

3. All remote access tools must be acquired through the standard Major Retailer procurement process, and the information technology group must approve the purchase.

4.2 The company’s Ramifications

Failure to use secure, supported remote access tools may expose Major Retailer to computer intrusion activity and could lead to loss of intellectual property, revenue, and/or reputation. It is the responsibility of each employee to protect the interests of Major Retailer while utilizing Major Retailer’s assets and information.
5.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Deliberate malicious activity involving theft or damage of intellectual property may be subject to criminal prosecution.

6.0 Definitions

<table>
<thead>
<tr>
<th>Terms</th>
<th>Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Challenge-Response:</td>
<td>A protocol where one party presents a “challenge” and the other must present a “response” to be authenticated.</td>
</tr>
<tr>
<td>Data loss prevention:</td>
<td>A system to identify, monitor, and protect data in use, at rest, and in motion from accidental or intentional transmission.</td>
</tr>
<tr>
<td>LDAP:</td>
<td>Lightweight Directory Access Protocol -- a protocol for querying and modifying directory services (often user authentication information).</td>
</tr>
<tr>
<td>Replay Attack:</td>
<td>The use of a previously recorded authentication session in order to obtain unauthorized access.</td>
</tr>
<tr>
<td>Remote access tool:</td>
<td>Any of a number of tools that provide remote access to a computer system “as if” the remote user were actually sitting in front of the computer.</td>
</tr>
<tr>
<td>Deepnet:</td>
<td>A two-factor authentication system consisting of something the user has (a “token”) and something he or she knows (the PIN).</td>
</tr>
</tbody>
</table>
Major Retailer

Mobile Security Policy

The company.

Mobile Security Policy

3.0 Overview
With advances in computer technology, mobile computing and storage devices have become useful tools to meet the business needs at Major Retailer Stores. These devices are especially susceptible to loss, theft, hacking, and the distribution of malicious software because they are easily portable and can be used anywhere. As mobile computing becomes more widely used, it is necessary to address security to protect information resources at Major Retailer Stores.

4.0 Purpose
The purpose of this policy is to establish an authorized method for controlling mobile computing and storage devices that contain or access information resources at Major Retailer Stores.

3.0 Scope
Major Retailer Stores employees, consultants, vendors, contractors and others who use mobile computing and storage devices on the network at Major Retailer Stores.

4.0 Policy
It is the policy of Major Retailer Stores that mobile computing and storage devices containing or accessing the information resources at Major Retailer Stores must be approved prior to connecting to the information systems at Major Retailer Stores. This pertains to all devices connecting to the network at Major Retailer Stores, regardless of ownership.

Mobile computing and storage devices include, but are not limited to: laptop computers, personal digital assistants (PDAs), plug-ins, Universal Serial Bus (USB) port devices, Compact Discs (CDs), Digital Versatile Discs (DVDs), flash drives, modems, handheld wireless devices, wireless networking cards, and any other existing or future mobile computing or storage device, either personally owned or Major Retailer Stores owned, that may connect to or access the information systems at Major Retailer Stores. A risk analysis for each new media type shall be conducted and documented prior to its use or connection to the network at Major Retailer Stores unless the media type has already been approved by the Desktop Standards and Support Team. The Desktop Standards and Support Team will maintain a list of approved mobile computing and storage devices.

Mobile computing and storage devices are easily lost or stolen, presenting a high risk for unauthorized access and introduction of malicious software to the network at Major Retailer Stores. These risks must be mitigated to acceptable levels.

Portable computing devices and portable electronic storage media that contain confidential, personal, or sensitive Major Retailer Stores information must use encryption or equally strong measures to protect the data while it is being stored.

Unless written approval has been obtained from the Vice President of Information Technology, databases or portions thereof, which reside on the network at Major Retailer Stores, shall not be downloaded to mobile computing or storage devices.
Technical personnel and users, which include employees, consultants, vendors, contractors, and students, shall have knowledge of, sign, and adhere to the Computer Use and Information Security Policy Agreement. Compliance with the Major Retailer Remote Access Standard, the Mobile Media Standards, and other applicable policies, procedures, and standards is mandatory.

5.0 Procedures
 Minimum Requirements:
 o To report lost or stolen mobile computing and storage devices, call the Computer Support at 616-878-2480. For further procedures on lost or stolen handheld wireless devices, please see the PDA Information and Procedures section.
 o Major Retailer Stores Desktop Standards and Support Team shall approve all new mobile computing and storage devices that may connect to information systems at Major Retailer Stores. Any non-departmental owned device that may connect to Major Retailer Stores network must first be approved by technical personnel such as those from Major Retailer Stores Desktop Support. Refer to the Mobile Media Standards for detailed information.
 o Submit requests for an exception to this policy to the Vice President of Information Technology.

6.0 Roles and Responsibilities
 Users of mobile computing and storage devices must diligently protect such devices from loss of equipment and disclosure of private information belonging to or maintained by Major Retailer Stores. Also, those with remote access privileges to Major Retailer Stores corporate network, will be responsible for ensuring that their remote access connection is given the same consideration as the user's on-site connectivity. Before connecting a mobile computing or storage device to the network at Major Retailer Stores, users must ensure it is on the list of approved devices issued by the DSS team.

The Computer Support must be notified immediately upon detection of a security incident, especially when a mobile device may have been lost or stolen.

The Information Technology Security Group is responsible for the mobile device policy at Major Retailer Stores and shall conduct a risk analysis to document safeguards for each media type to be used on the network or on equipment owned by Major Retailer Stores.

The Information Technology Division is responsible for developing procedures for implementing this policy. The Desktop Standards and Support Team will maintain a list of approved mobile computing and storage devices and will make the list available on the intranet.

7.0 Definitions

<table>
<thead>
<tr>
<th>Terms</th>
<th>Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>CD:</td>
<td>A compact disc (sometimes spelled disk) is a small, portable, round medium made of molded polymer (close in size to the floppy disc) for electronically recording, storing, and playing back audio, video, text, and other information in digital form.</td>
</tr>
<tr>
<td>DVD:</td>
<td>The digital versatile disc stores much more than a CD and is used for playing back or recording movies. The audio quality on a DVD is comparable to that of current audio compact discs. A DVD can also be used as a backup media because of its large storage capacity.</td>
</tr>
<tr>
<td>Flash Drive:</td>
<td>A plug-and-play portable storage device that uses flash memory and is lightweight enough to attach to a key chain. The computer automatically recognizes the removable drive when the device is plugged into its USB port. A flash drive is also known as a keychain drive, USB drive, or disk-on-key.</td>
</tr>
</tbody>
</table>
keychain drive, which looks very much like an ordinary highlighter marker pen, can be used in place of a floppy disk, Zip drive disk, or CD.

**Handheld wireless device:**
A communication device small enough to be carried in the hand or pocket and is also known as a Personal Digital Assistant (PDA). Various brands are available, and each performs some similar or some distinct functions. It can provide access to other internet services, can be centrally managed via a server, and can be configured for use as a phone or pager. In addition, it can include software for transferring files and for maintaining a built-in address book and personal schedule.

**Media Type:**
For the purpose of this policy, the term “media type” is interchangeable with “mobile device.” Not to be confused with media makes, models, or brands.

**Media Type Model:**
Refers to the brand of media device such as Sony, Treo, or IBM.

**Mobile Devices:**
Mobile media devices include, but are not limited to: PDAs, plug-ins, USB port devices, CDs, DVDs, flash drives, modems, handheld wireless devices, and any other existing or future media device.

**Modems:**
A device that modulates and demodulates information so that two computers can communicate over a phone line, cable line, or wireless connection. The connection talks to the modem, which connects to another modem that in turn talks to the computer on its side of the connection. The two modems talk back and forth until the two computers have no further need of either modem’s translation services.

**PDA:**
The Personal Digital Assistant is also known as a handheld. It is any small mobile hand-held device that provides computing and information storage and retrieval capabilities for personal or business use, often for keeping schedule calendars and address book information handy. Many people use the name of one of the popular PDA products as a generic term, such as Hewlett-Packard's Palmtop and 3Com's PalmPilot.

**Plug-In:**
Programs that can easily be installed and used as part of your Web browser. A plug-in application is recognized automatically by the browser, and its function is integrated into the main HTML file that is being presented. Among popular plug-ins is Adobe's Acrobat, a document presentation and navigation program that provides a view of documents just as they look in the print medium. There are hundreds of plug-in devices.

**Wireless Networking Cards:**
Mobile device for wireless internet connectivity from a laptop. This card allows mobile users the ability to access a secured connection to the internet via a specified vendor.

---

**Revision History**
2012-09-14 Initial Revision.
Major Retailer

Mobile Media Standard

1.0 Overview

As stated by the Mobile Security Policy, all mobile media devices used at the company must be tested, approved and standardized by the Desktop Support and Services team. All mobile media devices and their minimum requirements are listed below.

1. Tablets
   a. Requirements
      i. Windows based operating system
      ii. Minimum of 4 GB of RAM
      iii. Minimum 120 GB Solid State Drive
      iv. Minimum Intel Core i5 3337U – 1.8 GHz processor

2. Laptops
   a. Requirements
      i. Windows based operating system
      ii. Minimum 4 GB of Ram
      iii. Minimum 360 GB HDD
      iv. Minimum Intel Core i5 3320M – 2.6 GHz processor

3. Flash drives
   a. Requirements
      i. – Minimum 2 GB

4. CD ROMS
   a. Requirements
      i. – Minimum read/write capability
      ii. – Minimum 24x speed

5. DVD
   a. Requirements
      i. – Minimum read capability