Bring Your Own Device Security Issues and Challenges

Yong Wang†, Jinpeng Wei‡, Karthik Vangury†

College of Business and Information Systems†
Dakota State University
Madison, SD 57042
yong.wang@dsu.edu, kvangury@pluto.dsu.edu

School of Computing and Information Sciences‡
Florida International University
Miami, FL 33199
weijp@cs.fiu.edu

***Abstract*—As mobile devices become prevalent in workplaces, it also creates a unique environment, Bring Your Own Device, in enterprise networks. BYODs are extensions of corporate networks and thus it is essential to secure BYODs to protect enterprise networks. Security tools such as firewalls, anti-virus software, and anti-spam software have been widely used to protect corporate networks. Similar tools are also desired to protect BYODs. BYODs have many advantages, such as reducing companies' cost and increasing users' productivity. However, they also raise many security issues and challenges due to their unique security requirements. This paper summarizes threats and attacks on BYODs and reveals their security issues and challenges. The paper further compares existing BYOD solutions and presents a BYOD security framework that provides guidance for enterprises when adopting BYODs.**

***Index Terms*—BYOD, Security, Space Isolation, Corporate Data Protection, Security Policy Enforcement**

I. Introduction

Mobile devices, such as smartphones and tablets, have been widely used for personal and business purposes. According to a recent report from KPBC, the number of smartphone users has risen above a billion in Q3 2012 globally [1]. Gartner estimated that 1.2 billion smartphones and tablets could be sold in 2013 [2]. It is a 46 percent increase compared to the 821 million devices sold in 2012. However, when considering the 5.9 billion global mobile subscribers [3], smartphone and tablet adoption is still in early stage.

As mobile devices become popular, they are also becoming prevalent in workplaces such as corporate networks and campus networks. Traditionally, companies would provide mobile devices to their employees. However, as newer devices come out much faster than companies can afford to replace the existing ones, this is no more a feasible option. Many companies started to adopt mobile devices from employees. This has created a unique environment, **Bring Your Own Device** (BYOD), in enterprise networks. In a security survey by Courion, 69% of all enterprises indicate that their employees were using personal mobile devices to connect to the corporate networks [4]. As the number of employees using mobile devices increases, so does the risk that corporate data will be lost or released into the wild. A recent study carried out in the U.K. by security firm CPP found that over 50% of used mobile devices still contained large amounts of data from the previous owners [5]. This is in spite of the fact that 86% of consumers surveyed indicate that they made efforts to erase all personal data from their mobile units before selling or recycling them [5].

BYODs have many advantages, such as reducing companies' cost and increasing employees' productivity. However, BYODs also raise many security issues and challenges in enterprise networks [6]. One of the concerns is corporate data security. Theft and loss are two major threats of mobile devices. Thus, it is critical to protect corporate data stored on a BYOD. Further, BYODs are extensions of enterprise networks. Therefore, it is essential to secure BYODs and thus protect enterprise networks. A few BYOD solutions (mobile device management system and mobile virtual machines) exist and aim to address BYOD security. However, limitations and drawbacks are also found in these approaches. Given the number of reasons for using BYODs, administrators and IT professionals must look into security issues before adopting BYODs.

In this paper, we summarize security threats and attacks on BYODs and reveal their unique security issues and challenges in enterprise networks. We investigate and compare four current BYOD solutions. We further present a BYOD security framework that meets all the security requirements and provides guidance for enterprises when adopting BYODs.

The remainder of the paper is organized as follows: Section II summarizes security threats and attacks in mobile devices. Section III reveals security issues and challenges unique to BYODs. Existing BYOD solutions are discussed and compared in Section IV, followed by our BYOD security framework in Section V. Section VI concludes the paper.

II. BYOD Security Threats and Attacks

BYODs are the computing devices, such as smartphones, tablets, and PDAs, which are brought by employees and are able to connect to a corporate's network. As smartphones and tablets become popular in workplaces, the term BYOD is often used to refer to these mobile devices. In this paper, we

978-1-4799-2355-7/14/$31.00 ©2014IEEE

Threats and Attacks		Description
Sniffing		Tapping or eavesdropping, e.g., GSM A5/1 cracked
Spam		Email spam and MMS message spam, e.g., unsolicited MMS
Spoofing		Spoof *"Caller ID"* or MMS *"Sender ID"*, e.g., spoofed MMS messages from 611
Phishing		Steal personal information using a spoofed target mobile application
Pharming		Redirect web traffic to a malicious website and followed by more specific attacks
Vishing		Voice phishing by utilizing VoIP technique
Data leakage		Unauthorized transmission of data, e.g., mobile virus ZitMo
Vulnerabilities of Webkit engine		Vulnerability allowing attackers to crash user applications and execute code, e.g., the Webkit vulnerability revealed by CrowdStrike
DoS	Jamming	Jamming radio channel
	Flooding	MMS message flooding attacks and incoming phone call flooding attacks
	Exhausting	Battery exhaustion attack
	Blocking	Use smartphone blocking functions to disable smartphone

Table 1. Threats and Attacks on Mobile Devices

use BYODs to refer to mobile devices such as smartphones and tablets. BYODs include the following elements:

- They come pre-installed with a modern mobile operating system such as iOS, Android, or Windows Mobile.
- They support a carrier's networks (2G/3G/4G), Wi-Fi networks and Bluetooth.
- They are able to access the Internet. Internet accessibility is provided through either a carrier's networks or a local Wi-Fi network.
- They are capable of running third party applications downloaded from application stores through the Internet.
- They support MMS messages and have embedded sensors inside.

A. Threats and Attacks

BYODs are mobile devices and thus they are vulnerable to various threats and attacks like other mobile devices. These threats and attacks are summarized in Table 1 [7].

These threats and attacks are usually carried out by malware that disguises itself as normal mobile apps such as games, a security patch, or other desirable applications and is then downloaded to a mobile device. Mobile malware falls in three main categories: virus, Trojan, and spyware [8]. Trojan and spyware are the dominant malware in smartphones. According to Juniper's report in 2012, malware targeting the Android platform rose 3,324 percent in the last seven months of 2011 [8].

B. BYOD Vulnerabilities

A BYOD integrates many functions such as emails, calendars, notes and may include sensitive information related to organizations or personnel. Moreover, BYODs are also used for business and may carry critical corporate data. The sensitive information on a BYOD may include, but is not limited to

- Personal information such as home address, phone number, pictures, contact lists, etc.
- Correspondence business information such as emails, text messages, MMS messages, call logs
- Credit card information, secret credentials such as user names and passwords
- Files on flash memory or memory card
- Corporate documents such as word documents and spreadsheets
- Geographical location

The central data management of a BYOD is very attractive to hackers and it makes BYODs easy targets. BYODs are vulnerable to many threats and attacks as described in Table 1. The vulnerabilities of BYODs are due to the lack of confidentiality, isolation, and compliance on BYODs.

1) Confidentiality

BYODs may carry sensitive data such as corporate data. This data should not be stored on a BYOD in plaintext. It is essential to protect confidentiality of corporate data on a BYOD.

Further, it is not only essential to protect confidentiality of corporate data, but also important to monitor and reject unauthorized and illegal access of corporate data. Unauthorized access comes from insiders (employees or former employees) when they are not supposed to access corporate data. Illegal access comes from outsiders when they want to recover corporate data stored on a BYOD, e.g., malicious users try to steal data from a lost BYOD. Once data is downloaded to a BYOD, it is easy to make copies and transfer files from a BYOD to other mediums. Thus, unauthorized and illegal data access on a BYOD should be monitored and rejected. Encryption can be used to protect confidentiality of corporate data. However, novel cipher techniques should be explored to prevent unauthorized and illegal access on corporate data.

2) Isolation

BYODs are adopted for both personal use and business use. These two have different security requirements. When used

Challenges	Impacts and Countermeasures
Mobile devices are consumer products	Different groups have different perspective and security needs. Mobile device security tools should be flexible and configurable.
Mobile devices are platform-oriented	Multiple operating systems, e.g., Android and iOS, exist. Security software must be customized for each operating system and each version.
Mobile devices are a multiple entrance open system	Each entrance (Bluetooth or Internet) might be a potential back door for malware. Need to break the attack loop, e.g., malware detection, prevention, and removal.
Mobile devices are easy targets because of their central data management	A mobile device carries sensitive data, personal and banking information, in a central place. Encryption techniques and migrate data to cloud.
Mobile devices are resource-constrained devices and are easy to physically tamper	Security solutions must consider computational complexity and battery consumption. Add password or enable auto-lock, anti-theft technology.
Mobile devices are at high risks with embedded sensors inside	Smartphone sensitive data might be stolen and abused. Resource monitoring and intelligence to block illegal sensor access.
Mobile devices jeopardize business operations	It is difficult to audit and enforce security policies in a personal device. Isolate and enforce security policies at a higher security level on corporate data.
There is lack of security awareness among mobile users	Reluctant to update firmware and apply security patches. Education, smartphone security policy enforcement, and audit

Table 2. Security Challenges on Mobile Devices

for personal, BYOD owners look for the flexibility and convenience to decide what apps can be downloaded and what can be installed. However, when used for business, it is essential for organizations to ensure that the mobile devices are in compliance with the organizations' security policies. Space isolation is a desired feature and it makes it possible to apply different security policies on personal space and corporate space on a BYOD.

3) Compliance

BYODs are extensions of enterprise networks. However, it is hard to ensure that BYODs comply with enterprise security policies. A few BYOD solutions exist. However, they all have limitations when applying security policies on a BYOD. Further, BYODs are personal devices which are adopted for business use. It is impractical to manually audit an employee's personal device due to the ownership and also the large amount of BYODs. Alternative automatic options should be explored to enforce enterprise security policies on a BYOD [9].

III. BYOD Security Issues and Challenges

BYODs are mobile devices and thus they have similar security challenges like other mobile devices as shown in Table 2 [7]. Furthermore, BYODs also raise some security issues and challenges due to their dual purpose on personal and business use. These security issues and challenges are summarized as below.

A. BYOD Discovery

Because BYODs are part of an enterprise network, it is essential to monitor and track BYODs in such a network. BYOD discovery refers to the process of detecting BYODs in enterprise networks. BYOD discovery can be divided into two categories, agent-based BYOD discovery system, and scanning-based BYOD discovery system.

Agent-based BYOD discovery system requires an agent (a mobile app) installed on a BYOD. The agent is responsible for reporting the device status to a central network management system, e.g., Mobile Device Management (MDM) system. The agent is also used as a delegate on behalf of system administrators to enforce certain security policies on a BYOD. For example, the agent can be used to enforce password policy on a mobile device. The agent-based BYOD discovery system is easy to use and does not cause much communication overhead in an enterprise's network. However, it requires a mobile application to be installed on a BYOD first.

Scanning-based BYOD discovery system does not require any mobile apps installed on BYODs. Network scanning tools such as nmap can be used to detect BYODs based on their fingerprint. Since BYODs are usually connected to enterprise networks through Wi-Fi networks, it makes scanning BYODs possible. Scanning can also be based on Bluetooth interfaces on BYODs. However, the approach only works in small areas and is difficult to scale to large workspaces. Scanning-based BYOD discovery system does not require a mobile app to be installed on a device. However, scanning a network may take long time and it also adds extra traffic to an enterprise network. Our experiments with network scanning tools also show that scanning-based approach does not always guarantee that it will detect a BYOD in a network.

B. Corporate Space Isolation

BYODs are adopted for both personal use and business use. This naturally leads to separation of personal space and corporate space on a BYOD. BYODs are extensions of enterprise networks. Thus, BYODs must comply with an

enterprise's security policies. On the other hand, BYODs are also personal devices. Thus, individual users should also have the flexibility to choose and install mobile apps on their devices. Space isolation can solve this dilemma. Space isolation separates personal space and corporate space on a BYOD and thus makes applying different security policies on personal space and corporate space possible.

C. Corporate Data Protection

Corporate data includes business related data such as emails, contact list, calendar, and corporate documents. It is apparently essential to ensure security of corporate data. Corporate data protection has two aspects, i.e., protecting corporate data from outsiders, and protecting data from unauthorized and illegal access from both insiders and outsiders.

Theft and loss are two major threats for mobile device security. Many mobile forensic tools are available to collect data from mobile devices. Thus, it is critical to have corporate data encrypted and ensure it is not disclosed to outsiders if a BYOD is stolen or lost.

Corporate data encryption helps to protect data from outsiders. However, it does not help to protect data from unauthorized and illegal access by parties who have appropriate keys. For example, employees could copy and transfer corporate data downloaded to a BYOD to other mediums. If they have appropriate keys, they could figure out a way to recover encrypted data. Encryption is important to protect corporate data confidentiality. However, protecting data from unauthorized and illegal access is important to protect BYOD security too.

D. Security Policy Enforcement

BYODs are extensions of an enterprise's networks. Thus, it is essential to ensure that BYODs comply with the enterprise's security policies. The challenges that enterprises face in a BYOD environment include employees' unwillingness to backup data, lack of awareness of companies' security policies, lack of protection on corporate data, etc. Many of these issues can be resolved by auditing or enforcing a certain security standard on BYODs in an enterprise network. However, manually auditing on BYODs is time consuming and not practicable. Therefore, automatic ways to enforce security policies on BYODs should be explored. However, security policy enforcement on BYODs is challenging:

- Security policies are usually general statements which cannot be executed on BYODs.
- BYODs have different hardware, OS, applications, and versions. A security policy must be re-interpreted for each specific hardware platform.
- It is difficult for enterprise administrators and IT professionals to enforce and audit security policies for each individual smartphone subscriber. Practical automated security policy enforcement is desirable.
- Security policies may be changed and thus, must be updated constantly. Innovative approaches for security policy enforcement must be explored.

Significant discrepancy exists between BYOD security policy administration and security policy enforcement. Automatic security policy enforcement should be explored on BYODs in enterprises' networks.

IV. BYOD Solutions

A few solutions exist and aim to address BYOD security in enterprise networks. These solutions include virtual private networks, mobile device management system, mobile virtual machines, and Cisco BYOD smart solution.

A. Virtual Private Networks (VPNs)

In a typical enterprise network, Demilitarized Zone (DMZ) is usually used to protect internal networks. Users are also required to use Virtual Private Network (VPN) to connect to the internal network through the public Wi-Fi/cellular networks like 3G/4G. However, using DMZ or VPN does not help protect BYODs. First, BYOD owners are usually employees. They have no issues to connect their devices to the intranet. Second, VPN helps secure communication between BYODs and corporate networks. However, it does not help to protect data stored on BYODs.

B. Mobile Device Management (MDM)

Mobile Device Management (MDM) system is another option to secure BYODs. A MDM can be used to manage mobile devices and enforce certain security policies on mobile devices. A few MDM products have been available in the market, for example, FiberLink Maas360, Zenprise MobileManager, AirWatch MDM, and MobileIron. However, this approach has several limitations and drawbacks. First, MDM does not separate personal and corporate space on a BYOD. If a user has multiple roles in more than one organization, MDM system has issues to handle it. Each organization may have different security policies and MDM will have problems when handling conflicting policies. Further, MDM simply applies security policies on the whole device due to the lack of space isolation. Thus, BYOD owners will lose their flexibilities in their personal space if MDM is used.

C. Mobile Virtual Machines (MVMs)

Virtual machines have been widely used in desktop computers and cloud computing. They provide effective ways to separate space and data. As mobile devices become more powerful, developing virtual machines for mobile devices become practicable. Mobile Virtual machines (MVMs) can be used for separating personal space and corporate space in a BYOD [10], [11]. VMware Horizon Mobile is such an approach [12].

There are two options to develop virtual machines on mobile devices: heavy duty virtual machine and simplified lightweight virtual box.

Heavy duty virtual machines allow users to install multiple mobile operating systems on a mobile device. However, mobile devices are resource-constrained devices and may have issues to meet the high demand for computation power, memory, and disk space from multiple mobile OS instances. In addition, vendors may not be willing to support other mobile operating systems.

Simplified lightweight VMs require less computation and battery power. It does not provide multiple OS instances on a BYOD as heavy duty VMs can do. Instead, it utilizes lightweight virtualization technique to provide multiple virtual namespaces on a single OS instance, and each virtual namespace is isolated from one another. *Cells* is an example of such lightweight virtual machines [10].

A few prototype MVMs are available. However, this approach has not been widely used and commercialized.

D. Cisco BYOD Smart Solution

The Cisco BYOD Smart Solution provides the necessary infrastructure, including access points, controllers, security, and network management for BYODs [13]. Cisco's solution provides a foundation for BYODs when they are connected to a network. Different permissions (such as full access, partial access, Internet Only, and Deny Access) can be enforced on a BYOD. However, the solution does not provide any client support on BYODs, such as space isolation, and corporate data protection. Thus, the solution must be integrated with other approaches (e.g., MDM) to provide the desired security features on the BYODs.

Note that the solutions discussed here (such as VPNs, MDM, MVMs, and Cisco BYOD Smart Solution) must be used with other mobile security tools such as anti-virus software, and anti-spam software.

V. BYOD SECURITY FRAMEWORK

BYOD security is essential to protect enterprise networks. It is also challenging to secure BYODs due to their uniqueness. A few solutions exist and aim to address BYOD security issues. However, limitations are also found in these approaches (Section IV).

A. BYOD Security Requirements

A BYOD security solution must meet the following requirements:

1. Space isolation: it must be able to isolate personal space and corporate space on a BYOD so that different security policies can be applied.
2. Corporate data protection: corporate data should be encrypted when it is stored on a BYOD; Unauthorized or illegal access requests on corporate data should be monitored and rejected.
3. Security policy enforcement: it must be able to enforce enterprise security policies on BYODs and ensure that BYODs are in compliance with an enterprise's security policies.

These requirements provide the desired access control, confidentiality, and security policy management on BYODs. An ideal BYOD solution should meet all these three security requirements. Figure 1 shows a framework for BYOD security in an enterprise network which meets all these requirements. The framework includes two sides: enterprise side and BYOD side.

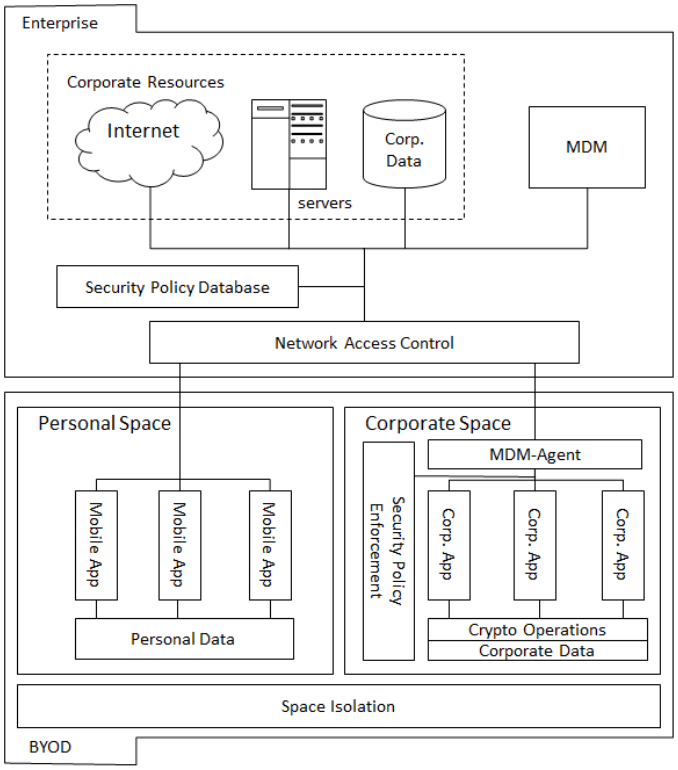

Figure 1. BYOD Security Framework

B. BYOD Security: Enterprise Side

Enterprise side includes various corporate resources, such as the Internet, servers, and corporate data and provides access control for BYODs to access these resources. The access requests are granted or declined based on enterprise security policies. Enterprise side also includes device management system, such as MDM, to manage BYODs.

Network access control provides access points for BYODs and grants BYOD access requests according to corporate security policies. Network access control needs to differentiate requests from personal space and corporate space on a BYOD. Using different certificates for personal space and corporate space is one option to differentiate these services.

Security policy database defines the enterprise's policies to handle BYODs. For example, how to handle access requests coming from personal space on a BYOD, what kind of BYODs are allowed to access the network, what is the cipher to be used, what is the key size, and so on.

MDM provides BYOD management capability. It has the functions to collect management information from a BYOD and enforce certain security policies on a BYOD.

C. BYOD Security: BYOD Side

BYOD side provides the functions to isolate corporate space, enforce security policies, and protect corporate data.

Space isolation provides the capability to separate personal space and corporate space on a BYOD. Space isolation is necessary for BYODs so that different security policies can be applied. Personal space includes employees' self-installed mobile apps and personal data. Corporate space includes corporate mobile apps and corporate data. Mobile apps and data in corporate space must comply with enterprise security policies. Ideally, personal space should not be able to access corporate resources, but may have limited access on certain resources such as the Internet. There might be some applications, such as SKYPE, that are desired for both personal and business use. Instead of sharing the application between personal space and corporate space, the applications should be installed separately in both to ensure the security of corporate data.

MDM-Agent is a mobile application that is installed in corporate space. MDM-Agent sends BYOD management information to MDM and acts as a delegate on behalf of system administrators to enforce certain security policies on a device. For example, MDM can issue a remote wipe command and wipe all the corporate data on a BYOD.

Security policy enforcement ensures that a BYOD complies with an enterprise's security policies. Security policies may include what crypto operations should be used, the size of the keys, and so on. A security policy database (SPD) is maintained in the corporate space. SPD includes information such as data type, security protocols, and keys.

Corporate data protection provides protection on corporate data. It can not only ensure that corporate data is stored in cipher text in storage, but also ensure that corporate data cannot be copied, or transferred illegally or without authorization. Crypto operations provides the desired cryptographic primitives (such as ciphers, hash functions, and digital signatures) to support corporate data protection.

D. BYOD Security Framework Implementation

BYOD security framework provides general guidance to adopt BYODs in an enterprise environment. Current solutions, such as MDM, mobile virtual machines, and Cisco Smart BYOD Solutions, could be integrated together to provide complete features to manage BYODs in an enterprise working environment. Further, current BYOD solutions focus on confidentiality of corporate data. Unauthorized and illegal data access on a BYOD should also be considered in a BYOD security solution.

VI. Summary

BYODs are extensions of enterprise networks. It is essential to protect BYODs and thus protect security of enterprise networks. BYODs are vulnerable to many threats and attacks like other mobile devices. BYODs may be even more attractive to attackers because they may carry critical corporate data. Security tools such as firewalls, anti-virus, and anti-spam have been widely used to protect enterprise networks. Similar tools are also desired to protect BYODs. A few solutions exit for BYOD security. However, limitations and drawbacks have been found in these solutions.

Securing BYODs has many challenges due to the dual purposes of personal use and business use on BYODs. An ideal BYOD solution must be able to separate corporate space from personal space and protect corporate data and monitor and reject unauthorized and illegal data access. Furthermore, it must also ensure that BYODs comply with an organization's security policies in an enterprise network.

References

[1] M. Meeker, "Internet Trends @ Stanford," 2012.

[2] Gartner Press Release, "Gartner Says 821 Million Smart Devices Will Be Purchased Worldwide in 2012; Sales to Rise to 1.2 Billion in 2013," Barcelona, Spain, 06-Nov-2012.

[3] ITU, "Key Global Telecom Indicators for the World Telecommunication Service Sector," Nov-2011.

[4] Courion Press Info, "69% of Enterprises Say Employees are Connecting Personal Mobile Devices to the Corporate Network; More Than One in Five Organizations Does Not Have a Policy in Place to Govern This Use," 26-Jul-2011.

[5] P. Wagenseil, "Half of Used Cellphones Still Hold Personal Data," *NBC News*, 22-Mar-2011.

[6] K. Miller, J. Voas, and G. Hurlburt, "BYOD: Security and Privacy Considerations," *IT Professional*, vol. 14, no. 5, pp. 53–55, 2012.

[7] Y. Wang, K. Streff, and S. Raman, "Smartphone Security Challenges," *Computer*, vol. 45, no. 12, pp. 52–58, Dec. 2012.

[8] Juniper Neworks, "2011 Mobile Threats Report," 2012.

[9] R. Xu, M. Park, and R. Anderson, "Aurasium : Practical Policy Enforcement for Android Applications," in *USENIX Security 12*, 2012.

[10] J. Andrus, C. Dall, A. Van Hof, O. Laadan, and J. Nieh, "Cells : A Virtual Mobile Smartphone Architecture Categories and Subject Descriptors," pp. 173–187, 2011.

[11] K. Barr, S. Deasy, and C. Newell, "The VMware Mobile Virtualization Platform : is that a hypervisor in your pocket ?," pp. 124–135.

[12] VMware, "VMware Horizon Mobile," 2013. [Online]. Available: http://www.vmware.com/products/desktop_virtualization/mobile/overview.html.

[13] Cisco Systems, "BYOD Smart Solution," 2013. [Online]. Available: http://www.cisco.com/web/solutions/trends/byod_smart_solution/index.html.