Journal of Information Technology Management

ISSN #1042-1319

A Publication of the Association of Management

MOBILE DEVICE SECURITY ISSUES WITHIN THE U.S. DISADVANTAGED BUSINESS ENTERPRISE PROGRAM

MARK A. HARRIS
UNIVERSITY OF SOUTH CAROLINA
maharris@sc.edu

KAREN P. PATTEN
UNIVERSITY OF SOUTH CAROLINA
pattenk@sc.edu

ABSTRACT

This paper reports on the results of a mobile device security awareness and practice survey of one special type of small business referred to as *Disadvantaged Business Enterprises (DBEs)* within the U.S. Department of Transportation. As government contractors, DBEs have access to government information systems. With recent cyber-attacks on large corporations through their less secure subsidiaries, it is essential that DBEs take security precautions and do not become an illegitimate point of entry to government systems. This paper discusses the roles, responsibilities, and IT security weaknesses within the U.S. DOT and surveys 1088 DBEs about their mobile device security and mobile device business usage. Results demonstrate that the majority of DBEs failed to adequately address even the most basic mobile device security practices, potentially exposing government systems, which are already poorly secured. This paper provides a list of basic mobile device security recommendations for immediate DBE adoption.

Keywords: mobile device security, small/ medium-sized businesses, U.S. DOT, Disadvantaged Business Enterprises (DBEs)

INTRODUCTION

Business mobility is changing the way business is conducted in small, medium, and large enterprises, the military, and government agencies. Business mobility gives business employees the capability to transact business anywhere and anytime, to collaborate in real time, and to have access to critical data at the right time in the right place. The expansion of business mobility in recent years is due to the globally accepted use and proliferation of mobile devices, such as smartphones and tablets. However, the advantages these devices bring come with increased information security risk and ignoring that risk can be detrimental to the business [10].

Nearly 60% of all phones sold in 2013 were smart phones [7]. Smartphone sales are expected to reach nearly two billion units in 2014, while tablet sales are predicted to reach just over 250 million units and outsell PC's by 2015 [8]. Google's Android operating system, the most popular, was chosen for nearly 80% of all smartphones sold in 2013, compared to just 16% for Apple's iOS, 3% for Microsoft's Windows Mobile, and 2% for Blackberry [7]. With smartphones and tablets increasing in popularity, malware has also significantly increased, particularly for the Android platform, which saw a 600% increase in 2013 compared to the year before [11]. Of all detected malware in 2013, 99% was written for Android [4]. However, Apple iOS applications are not without risk. In a recent report on Google Play's and Apple App Store's top 100 paid apps and top 100 free apps, Appthority [3] reported that iOS apps were found to be more risky than Android apps.

Most businesses are small and medium enterprises (SMEs). SMEs are the driving force behind economic growth and have a large impact on both the local and national economies [28]. One particular type of SME is the Disadvantaged Business Enterprise (DBE), which is a small business contractor within the U.S. Department of Transportation (U. S. DOT) [26]. A DBE firm is owned and controlled by socially and economically disadvantaged individuals. Each state and local transportation agency that receives Federal dollars from the U.S. DOT must establish DBE participation goals and certify DBE firm eligibility to participate in U.S. DOT assisted projects. Because DBEs are considered contractors for the U.S. DOT, they have special, but limited, access to government information systems. The U.S. DOT has over 450 information systems that are used for critical operations such as preventing unqualified drivers from obtaining driver's licenses, identifying safety defects in vehicles, and ensuring safe air traffic control [17]. DBE access to government systems is a potential risk if a perpetrator were to gain access though insecure DBE systems, as in the case where Target Corporation's systems were compromised through a contractor with special, but limited access. The Target breach compromised the data of millions of customers. A DBE breach into government systems could potentially be much worse. Because of the popularity of mobile devices used for business purposes and the potential risk to government systems through a DBE contractor, the purpose of this study was to investigate DBE mobile device security and DBE usage of mobile devices for government contract business purposes.

The next section provides a more detailed description of the DBE program, followed by a section that describes DBE security practices, including responsibilities and known weaknesses within the U.S. DOT. Next, current smartphone and tablet security issues are documented. The methodology section describes an online survey and describes the DBE participants. The results and then the discussion sections then outline the current state of security with DBE smartphone and tablet use followed by a DBE recommendation section. The next to last section summarizes the need for DBEs to implement mobile device security practices followed by the conclusions, which summarize the potential risk of the use of smartphones and tablets by DBEs.

DISADVANTAGED BUSINESS ENTERPRISES (DBES)

The U.S. Department of Transportation participates in the Federal Government's program to increase the participation of minority-owned and women-owned small businesses. The U. S. DOT program is called the Disadvantaged Business Enterprise (DBE) Program [26]. At least ten percent of all federally-assisted highway and transit program funds must go to DBE's, which is a statutory provision first established in 1983 by the U. S. Congress. The Office of Small and Disadvantaged Business Utilization (OSDBU) distributes billions of assistance dollars annually to help finance thousands of U.S. DOT projects across the country.

State and local transportation agencies that receive U.S. DOT Federal dollars are responsible for establishing narrowly-defined annual goals for DBE subcontracting participation, to certify the eligibility of all DBE's who participate in U.S. DOT-assisted projects, to review the scopes of anticipated large prime contracts throughout the year, and to evaluate their U.S. DOT-Federal contracts throughout the year to make sure they meet their overall agency goal [26]. Three major U.S. DOT operation administrations, the Federal Highway Administration (FHWA), the Federal Transit Administration (FHA), and the Federal Aviation Administration (FAA), participate in the DBE program.

To become a certified DBE, small for-profit enterprises must first be defined to be a small business and, secondly, they must be at least 51% owned, managed, and controlled by socially and economically disadvantaged individuals [26]. These individuals include African Americans, Hispanics, Native Americans, Asian-Pacific, Subcontinent Asian Americans, and women. Other individuals can also qualify as socially and economically disadvantaged on a case-by-case basis. Each state has a department that is responsible to qualify eligible DBEs by reviewing resumes of principal owners, establishing the firm's financial capacity, visiting the firm premises, conducting on-site visits and personal interviews, and reviewing licenses, stock ownership, equipment, bonding capacity, and work completed [26].

DBE INFORMATION SECURITY

As contractors for the U.S. DOT, DBEs are required to follow Federal laws and regulations. However, the U.S. DOT also has obligations to support DBE contractors when dealing with information technology and security issues. The next sections describe the information security responsibilities of the DBEs and U.S. DOT as well as specific information security weaknesses described in recent security audits.

DBE Information Security Responsibilities

According to the Electronic Code of Federal Regulations [5], small business owners who are DBE contractors are responsible for the security of the information technology that they may use to physically or electronically access U.S. DOT information and networks. The Office of Management and Budget (OMG) Circular A-130 [18] defines information technology (IT) to include the acquisition, storage, manipulation, management, control display, switching interchange, transmission, or reception of data or information as well as major applications and general support systems. The DBE contractor is also governed by the provisions of the Privacy Act of 1974.

Each DBE contractor must also develop, provide, implement, and maintain an *IT Security Plan*, which should ensure appropriate security of all IT resources [5]. The Federal Information Security Management Act (FISMA) of 2002 and the E-Government Act of 2002 describe the related Federal laws. In addition to submitting the IT Security Plan, the contractor must also submit a *Continuous Monitoring Plan* that includes the configuration management process for the information systems and its components, the security impacts of any changes to the system, and the assessment of the security controls. According to the OMB Circular A-130 [18], the FISMA Act of 2002, and the National Institute of Standards and Technology (NIST) requirements, the contractors must also provide *annual IT security training* for any employees involved in the contract. The contractor must also notify the Contracting Officer when any employee who has access to government information systems or data is hired or terminated.

U.S. DOT Information Security Known Weaknesses

In an audit report, issued November 2013, the Office of Inspector General (OIG) [17] described persistent weaknesses in the controls used by the U.S. DOT to protect and secure its information systems. In summarizing the findings, the first weakness identified was that procedural guidance was not detailed enough and that the U.S. DOT's 13 operating administrations (OAs) had yet to complete information security management procedures, such as continuous monitoring. Secondly, the U.S. DOT's enterprise-level controls were not adequate to ensure all contractors received security training, personnel with significant security responsibilities received specialized training, all possible security incidents are detected and reported, and configuration baselines and changes are appropriately managed. Since 2008, the U.S. DOT has not known how many contractors it employs and does not know how many completed or need to complete required annual security training. Thirdly, the U.S. DOT's system-level controls remain insufficient to protect system security and ensure systems can be recovered in the event of an emergency shutdown. For example, OAs had not implemented controls for identifying and managing the risks associated with their systems, such as user identity verification and access control. Lastly, the U.S. DOT lacked an effective process for timely remediating of security weaknesses. The overall conclusion of the audit report was that the U.S. DOT was vulnerable to serious security threats due to these and other deficiencies [17]. Due to the lack of security and control in the U.S. DOT, any penetration into its more than 450 information systems could have major implications, particularly to air traffic control systems.

National Institute of Standards and Technology Mobile Device Security Guidelines

Recognizing Federal employee benefits of flexibility and efficiency when using smartphones and tablets, the National Institute of Standards and Technology (NIST) updated its earlier 2008 mobile computing guidelines with *NIST 2013 Special Publication 800-124: Guidelines for Managing the Security of Mobile Devices in the Enterprise* [16].These guidelines are designed for the centralized management of mobile devices, including the use of MDM systems. However, the guidelines are not useful for very small businesses that do not use MDM systems. While MDM systems provide stronger security, many smaller businesses may choose to not use it because of the added cost per user or the lack of technical resources. NIST recognizes that the guidelines are not a blanket solution for everyone and states that not all organizations will need all security services listed. In these cases, NIST recommends that government agencies and their contractors should instead select security components necessary for each organization's environment [16].

MOBILE DEVICE SECURITY ISSUES

Unlike most PCs that use Microsoft Windows or Apples OS X, mobile devices use different operating systems (OSs). The two most popular, discussed in this paper, are Google's *Android* and Apple's *iOS*. These two platforms account for nearly 80% of all smartphone and tablet devices worldwide [25].

Mobile Applications, Markets, and Malware

Mobile device application malware has increased over 600% from 2012 to 2013 [11]. Ninety-two percent of all known malware has been written for the Android operating system [12]. Juniper also reports that 73% of known malware exploits SMS text messages at an average profit of $10 per text for the perpetrator.

Many legitimate applications, including free applications, are not considered malware, but may also cause problems. These legitimate applications pose a risk whenever they track location, access address books or contacts, or request or gain access to account information. Mearian [15] described several legitimate free applications that also could potentially leak corporate data. Free applications were three times more likely to track location and 2.5 times more likely to access address books than paid-for applications [15]. Free applications requesting access to account information doubled from 2012 to 2013.

One of the major differences between Android and iOS devices are the applications markets available to each. Apple has more control over applications for iOS devices because they have only one market, the *App Store*, which had over one million applications available for download as of late 2013 [1]. Google's *Google Play* market beat Apple to the one million apps mark in July 2013 [27]. Google Play now experiences over 2.5 billion downloads every month and has seen nearly fifty billion applications downloaded since its inception in 2008 [21]. However, Android does not limit users to the Google Play market. Android users are free to download apps from 3rd party markets as well. Over five hundred 3rd party Android application markets exist worldwide. Many of these 3rd party Android markets have low levels of accountability or oversight and are known to host malware [12]. Of those markets known to host malware, 60 % of them originate from either China or Russia. However, not all 3rd party markets are considered unsafe. For example, Amazon's *App Store for Android* is considered safer than Google's Google Play market [6].

Android and iOS Platforms

Another major difference in iOS and Android is that the Android platform is far more fragmented than iOS, meaning there are many versions of the operating system still in use. For example, as of October 2014, 47% of iOS devices had the latest iOS 8 version and 47% had the previous iOS 7 version [2], but only 24% of Android devices had its latest version, KitKat 4.4 [9]. At the time of this writing, it had only been one month since iOS8 was officially released [1] and one year since KitKat 4.4 was officially released. The problem with fragmentation is that the newer versions of the operating system are considered more secure, since they address known security vulnerabilities at the time they are introduced. Therefore, older versions still in use are less secure than newer versions. Juniper [12] reported that 77% of Android threats could be eliminated if all devices had Jelly Bean version 4.2, the latest version at the time of the report. As of mid-2013, only four percent of Android devices were version 4.2. Since then, two new versions of Android have been released, Jelly Bean 4.3 and KitKat 4.4. As of October 2014, 53% of Android devices have version 4.2 or higher. A large amount of existing Android devices (11.4 %) still use Gingerbread (released 2010 - 2011), 9.6% use Ice Cream Sandwich (released 2011 – 2012), and 25.1% use Jelly Bean 4.1 (released 2012). With the strongest security in the later versions, it is important to upgrade the operating system when prompted and upgrade the device when necessary to keep up with the current versions of the operating systems [12].

To address the fragmentation problem, Google changed the way upgrades are performed with the latest KitKat 4.4 version. Prior to KitKat, previous version upgrades had to go through Google, handset manufacturers, smartphone product lines, and then the wireless carriers before becoming available to the end user [24]. Because upgrades are not mandatory, any of those vendors involved in the upgrade process can decide the upgrade is not necessary, thus keeping the upgrade from reaching end users. Plus, it is in the best interest of carriers not to upgrade the operating system to the latest version in order to increase sales of new devices. KitKat changes the whole process by changing the operating system so that upgrades can be pushed directly to users through the Google Play market, thus eliminating the middle players [24]. Over time, as users upgrade devices to KitKat and newer versions, the fragmentation problem will become less serious.

Jailbreaking and Rooting

The process of using software to purposely hack one's own device to remove security restrictions is known as *jailbreaking* on iOS devices and *rooting* on Android devices [14]. While the procedures are technically different, the end result is that users can bypass security restrictions to gain full control of their devices. Since iOS devices restrict users the most, iOS users have the most to gain from jailbreaking their devices. For example, a jailbroken iOS device is no longer limited to downloading apps from only the Apple App Store. A jailbroken iOS device can download non-Apple-approved apps from 3rd party app stores. Users of jailbroken and rooted devices can also remove vendor-loaded applications, known as bloatware, which usually cannot be uninstalled. Other popular user benefits of jailbreaking and rooting include the ability to transfer applications, application data, and settings to new devices, create custom desktop environments, install illegal pirated applications, and upgrade to the latest operating system without vendor or handset restrictions. Jailbreaking or rooting devices has become a popular and risky trend. Malenkovich [14] estimated that between fifty to ninety percent of users opt to jailbreak or root their devices.

Since some of the primary reasons for jailbreaking or rooting are to participate in risky activities, including downloading pirated applications or downloading from 3rd party markets, users who jailbreak or root their devices are also more at risk for malware. The reason iOS forbids downloading from 3rd party markets is to minimize the security risk, but one primary reason iOS users jailbreak their devices is to download from 3rd party markets. Jailbroken and rooted devices should not be allowed on corporate or small business networks, plus downloading apps from markets other than Google Play, Apple's App Store, Amazon, and a few vendor markets should be avoided by most users. End users need to be more security-conscious because the security is no longer a part of the operating system on a jailbroke or rooted device.

Wi-Fi Networks

Although business employees using laptops have accessed Wi-Fi hot spots (wireless networks) for years before smartphones and tablets were commonly used, today, business employees consider Wi-Fi to be essential for smartphones and tablets. Because mobile device users pay carrier fees for cellular network data usage, "free" Wi-Fi is a popular option for accessing the Internet whenever Wi-Fi is available. However, Wi-Fi has its own security vulnerabilities. The three primary wireless security protocols, WEP, WPA, and WPA2, can all be easily cracked [13]. The first security protocol, WEP, is the weakest and should not be used under any circumstances. WPA originally was introduced to fix vulnerabilities from WEP protocols. WPA2 then expanded these security capabilities. When WPA and WPA2 were first introduced, they were thought to be immune from attack. However, as Knox reported [13], both have succumbed to multiple successful attack variants.

Using Wi-Fi with one of the built-in security protocols has risk, but using Wi-Fi with no security protocols is very risky. Many public "free" Wi-Fi hot spots allow access to open Wi-Fi networks, but do so with no security protocols. No security protocol makes it easy for perpetrators to use man-in-the-middle attacks to snoop on everything unsuspecting users do on their devices. While using no security protocol is the most dangerous, using Wi-Fi in public places even with security protocols is also dangerous and still subject to attacks. To improve security using Wi-Fi on untrusted networks, users should use virtual private networks (VPNs) to access the Internet at all times [13].

Mobile Device Management (MDM)

A difficult problem faced by enterprises today is managing the security of mobile devices, both corporate-owned and bring-your-own-devices (BYOD). BYOD devices are employee-owned devices that are used for both personal and business use. The complexity of managing these devices comes from the diversity of devices and their related operating systems. A single corporate network may include Android, iOS, Windows Mobile, RIM Blackberry, and other operating systems. Within those operating systems, there may be multiple versions of each operating system, as with the fragmented Android operating systems. Another problem is the presence or mixing of personal applications and data along with business applications and data on the same device.

Mobile Device Management (MDM), a policy and configuration management software tool for mobile devices, is an enterprise mobile solution for securing and enabling enterprise users and content [20]. Available features for each individual vendor's MDM may vary, but minimum features should include password management, remote data wipe, data encryption, jailbreak/root detection, data loss prevention, remote configuration, remote operating system and application updating, remote inventorying, and remote control [22]. A fully featured MDM can also manage all of the popular operating systems, devices, and OS versions. Depending on how an organization wants to secure its mobile devices, other options are also available, such as preventing the use of the camera and/or video recorder or preventing unauthorized application downloads. Another available feature of MDMs is Mobile Application Management (MAM), which manage applications from a variety of available security solutions. Minimum MAM features include application whitelists and blacklists, enterprise application stores, application security, and data wipe by application [22].

Two primary types of MDM system implementations include those installed in-house or those hosted on the cloud. In-house installations are typically controlled by in-house IT professionals. Cloud-based installations can be controlled by in-house IT professionals or outsourced to a 3rd party cloud vendor. There are many vendors available that can manage as little as a few devices to thousands of devices, depending on the need [22].

Dual Persona

A relatively new security solution for mobile devices in the workplace is the creation of a *personal environment* and a *work environment* on a single device, also known as 'dual persona [23].' The personal and work environments are securely kept separate from one another. In this way, business environment applications and data are isolated and can be kept safe from more risky applications in the personal environment. The enterprise can use MDM and MAM to manage the business environment and leave the personal environment alone. If an employee leaves the enterprise, MDM can be used to wipe the business environment clean of business data while leaving the personal environment as it was. Dual persona can be enabled through mobile virtualization with two operating systems sharing the same device or through a segregated business container on one operating system [23]. Most enterprise applications in the business environment can be designed to communicate with one another and be centrally managed. Other features may include encrypting, cutting and pasting to only the work environment with enterprise-approved applications, and preventing business email attachments from being opened in personal applications [23].

Mobile Device Security for SMEs and DBEs

Although security threats from smartphones and tablets are a concern for all users, small businesses face unique challenges when securing these devices. Unlike devices used strictly for personal use, devices used within small businesses may also contain business or customer data, which necessitates more extensive security safeguards. Unlike larger enterprises, a small business may not have the resources to hire a technology specialist or purchase security software to mitigate these risks [19]. The reality of these threats and the potential impact on small businesses points to the need for small business owners to be aware of the security concerns before making decision about smartphones and tablets in the workplace. The reality of the risk to Federal information and data used by DBEs in the course of their contractual work further increases the need to address security concerns.

The 2013 NIST-issued guidelines for mobile device security [16], provides centrally managed security recommendations for Federal agencies and Federal contractors. Although not all security services listed by NIST are relevant to DBEs, many security recommendations are, such as requiring a password/passcode to access the device, avoiding risky app markets, and utilizing VPNs over public or open Wi-Fi networks. A better match for improving DBEs' security capabilities is a list developed by Harris and Patten [10], consisting of eighteen recommended mobile device security components designed for small and medium enterprises with limited resources. Unlike the NIST guidelines, these guidelines make suggestions that can be used by smaller businesses with minimum or no IT staff and no centralized management (MDM).

METHODOLOGY

DBEs have potentially increased mobile device security risks and the popularity of mobile devices used for business purposes increases the potential risk to Federal systems through a DBE contractor. An online survey was developed to investigate DBE usage of mobile devices for government contract business purposes and current DBE mobile device security practices, an online survey was developed. The eighteen recommended mobile device security recommendations [10] along with associated security components from the NIST guidelines [16] were used to ascertain current DBE mobile device security practices.

Participants

The SME mobile device security online survey was sent to 30,788 DBEs representing U. S. DOT contractors in 43 states in early 2014. A total of 1088 complete responses were collected for a 3.5 percent response rate. DBE contact information was obtained from the U.S. DOT's Website, where certified DBEs are listed by state membership. Of the collected responses, the average DBE size was seventeen employees. CEOs and/or owners of a DBE accounted for 86% of the responses while presidents and vice presidents accounted for 7% of the responses, and other management accounted for 5% of the responses. The remaining 2% came from other employees with knowledge of mobile security situation within the business. Sixty percent of the surveyed DBE firms had no IT professionals on staff. Of those with at least one IT professional, the business averaged three IT professionals. The DBE business application accessed with mobile devices the most was e-mail (95%), followed by scheduling/calendar (73%), business banking (27%), accessing customer data (23%), and accepting payments (11%).

Each participant was asked if their business allowed the use of smartphones, tablets, and laptops/PCs. Depending on the devices used within a business, each participant was asked a series of security questions. A typical smartphone was defined for participants as phones with touch screens that allowed users to download and install applications from markets, citing Apple's iPhone, Samsung's Galaxy, and Motorola's Droid as examples. Tablets were defined as wireless portable computers with touchscreens that allowed users to download and install applications from markets, citing Apple's iPad, Google's Nexus, and Amazon's Kindle as examples. A typical PC was defined as a personal computer, such as a desktop computer, that has a larger box-like processing unit and large monitor. PCs typically run operating systems like Windows, Mac OSX, or Linux. Laptops were defined as portable computers that are larger than tablets and typically run PC operating systems, like Microsoft Windows or Mac OSX.

RESULTS

The NIST mobile device guidelines [16] stated the importance of having security policies in place that addressed mobile devices. Only 25% of those surveyed had such a security policy in place, although a much higher percentage of these businesses allowed mobile devices for business use, as summarized in Table 1. While laptops and personal computers (PC) were not considered mobile devices within this survey, the data is included where appropriate for comparison purposes. Table 1 also summarizes which type of devices DBEs used for business purposes. As expected, most DBEs reported their employees used laptops/PCs and smartphones. Tablets, however, were used much less, with only half of the DBEs reporting tablet usage. Most DBEs allowed smartphones to be used for business purposes.

Table 1: DBE Usage of Devices for Business Purposes

Device Type	Allowed Use	Used for Business Purposes	Business-Issued	BYOD
Smartphone	93%	88%	51%	65%
Tablet	67%	50%	30%	50%
Laptop/PC	95%	92%	63%	56%

When it comes to business-issued devices versus bring-your-own-device (BYOD), some enterprises find it easier to manage business-issued devices because they can make sure they all the mobile devices have the same operating system, are similar models, or come from the same vendor. With business-issued devices, enterprises also find it easier to enforce policies about device usage and application installation. This approach often results with employees using two mobile devices, one restricted to business use and one for personal use. When BYOD devices are allowed for work purposes, the business faces additional risks because of the variety of devices and their multiple operating systems from multiple venders. Even within similar operating systems, there could still be various versions, especially with the fragmented Android operating systems. Table 1 also shows how many surveyed DBEs allowed business-issued and BYOD devices, with many enterprises allowing both. One previously discussed security solution, for both business-issued and BYOD devices, is mobile device management (MDM). However, only 8% of DBEs surveyed used MDM software.

The various operating systems used on DBE devices are summarized in Table 2. It was expected that Apple's iOS would dominate the tablets because Apple's iPad was first to the market and enjoys a higher market share. Apple's iOS also significantly led the DBE business use of smartphone category too, which was not expected. This was because Google's Android has steadily gained market share over Apple's iOS, taking the market lead in 2012 and becoming the lead-selling smartphone operating system. It is apparent that over half of the DBEs surveyed have iPhones, which is good for security if not jailbroken, since iOS is considered a more secure platform.

When it comes to protecting their devices, DBEs failed to properly secure their mobile devices with the most basic security features, such as antivirus software. As summarized in Table 3, only 40% installed antivirus software on their non-iOS smartphones and less than half did on their non-iOS tablets. Since antivirus software is not available for Apple's iOS, only non-iOS devices were included in this table, such as Google's Android or Microsoft's Windows Mobile. Also, another very disturbing result is that nearly one in ten users failed to install antivirus software on their laptops\PCs. Since personal computers are not new technology, like smartphones and tablets, it is disappointing that not everyone realizes the importance of antivirus software on a laptop/PC.

Table 2: Device Operating Systems

Operating System	DBE Use		
	Smartphone	Tablet	Laptop/ PC
iOS	51%	70%	N/A
Android	32%	16%	N/A
Windows	0%	0%	85%
Mac OSX	N/A	N/A	14%

Table 3: Use of Security Safeguards

Security Safeguard	Installed		
	Smartphone	Tablet	Laptop/ PC
Antivirus	40%*	49%	91%
Authentication	57%	64%	82%
Data Wipe	28%	29%	13%
Security Suite	30%	34%	78%

* Responses do not include iOS devices

DBEs also failed to adequately use some form of authentication to access the device as shown in Table 3. Over 40% of smartphone users and over 35% of tablet users failed to use any form of authentication, such as a password or swipe pattern. If usernames and passwords for applications like e-mail are stored on these devices, there is nothing to stop an unauthorized user who has the device from accessing business emails.

Data wipe is another critical security feature because enterprises can wipe data from the device if it is lost or stolen. Data wiping features for mobile devices usually come in security suites that also contain other features such as antivirus software, safe browsing, and even GPS location for lost devices. The use of security suites and data wipe for mobile devices was very low for the DBEs surveyed. The only exception was that nearly 80% of the DBEs used security suites for laptops and PCs. However, the security suites for PCs rarely contained the data wipe feature, as shown in Table 3 where only 13% used the data wipe feature usage. It is recommended that data wipe be used for laptops although it is generally not needed for stationary desktop PCs.

Potentially DBE risky behaviors, summarized in Table 4, had mixed results. The most potentially risky behavior was the use of 3rd party app markets, where nearly 35% of DBEs installed software from these markets. Third party markets are risky because they often do not have a strong vetting process for their application developers and submitted applications, thus allowing more malware on the market. Another problem is allowing applications to store authentication credentials. If a perpetrator has possession of a mobile device and gains access, perhaps because of no logon authentication requirement, he or she would have access to accounts with stored credentials, such as business emails, calendar, Facebook, and Twitter.

Lost or stolen devices open the door for these types of attacks, allowing easy entry for devices with no authentication requirement and with stored app credentials. Over one in ten DBEs using smartphones had devices stolen or lost as shown in Table 4, solidifying the need to use secure credentials, backup, data wipe, and GPS device locating. Jailbreaking or rooting a device is also very risky behavior, but this result was better than expected. Only 3% of DBEs using smartphones and 2% of DBEs using tablets admitted to jailbreaking or rooting their devices.

Table 4: Potentially Risky Behaviors

Risky Behaviors	DBE		
	Smartphone	Tablet	Laptop/ PC
Installed software from 3rd party app markets	34%	35%	N/A
Allowed apps to store authentication credentials	31%	33%	52%
Lost or had device stolen	13%	3%	5%
Jailbroke or rooted device	3%	2%	N/A

Many employees use Wi-Fi at home, work, and in public places to save on cellular data costs. Wi-Fi connections in public places cannot be trusted and are often unprotected networks, increasing the risk for unsuspecting Wi-Fi users. Table 5 shows that over 70% of DBEs used Wi-Fi in public places. The best way to protect a mobile device using Wi-Fi in public is to use a virtual private network (VPN). However, only 15% of smartphone users, 18% of tablet users, and 24% of laptop/PC users used VPNs. As a result, those DBEs not using VPNs have a greater risk that their device will be compromised.

Table 5: The Use of Wi-Fi on Public Networks

Wi-Fi Network Use	DBE		
	Smartphone	Tablet	Laptop/ PC
Use Wi-Fi on public networks	70%	77%	64%
Use VPNs over Wi-Fi	15%	18%	24%

DISCUSSION

Further analysis of the data indicates extreme risk for some DBEs. Of those who indicated they had experienced a lost or stolen smartphone, 44% of those devices did not require any access authentication. Of those respondents who reported lost or stolen smartphones, 32% allowed applications to store usernames or passwords. Combining all three, 14% indicated that they had experienced a lost or stolen smartphone, did not use access authentication, and allowed applications to store usernames and passwords. Any unauthorized person possessing those devices under those circumstances would have full access to the applications with stored credentials.

Additional analysis highlighted another alarming combination of inadequate security practices. Of those DBEs that reported they downloaded smartphone application software from 3rd party markets, only 33% of them reported they used antivirus software. For tablets, only 38% reported using antivirus software while downloading apps from 3rd party markets. Since most of the mobile device malware is from 3rd party markets, it is essential to use antivirus software, at the very least. Those DBEs downloading from 3rd party markets without using antivirus software are at extreme risk of malware attacks. Also of concern are those who reported jailbreaking or rooting their smartphones. While only a small percentage reported doing so, of those that did, only 53% reported using antivirus software. Since a jailbroken or rooted device removes many security restrictions from the operating system, these devices are more at risk for malware attacks.

Most DBEs reported using their mobile devices for business purposes including business from Federally-funded U.S. DOT contracts. Therefore, it is essential that DBEs protect their business data and information on mobile devices. However, the results of this survey indicate that most DBEs failed to secure their mobile devices, potentially exposing government data and information to unnecessary risks. Currently, DBEs used mobile devices with a mixture of operating systems, although Apple’s iOS and Google’s Android were the most common. DBEs also used a mixture of smartphones and tablets, both business-issued and BYOD.

The security shortcomings come from a variety of areas, including the lack of antivirus or security suites in devices that allowed such products. While these security features pertain to non-iOS device users, iOS users also failed to properly secure their devices. Far too many DBEs failed to require proper authentication to access the device and failed to use data wipe features in the case of compromised or lost devices. They also increased risk by allowing apps to store credentials and downloading apps from 3rd party markets. Perhaps the most risky security practice identified by DBEs is the use of public Wi-Fi without using a VPN. The combination of all of these mobile device security flaws leads to the conclusion that DBEs fail to properly secure their mobile devices. In a society where hackers are to known to go after the weakest links to penetrate security, mobile devices for DBEs could very well be that weakest link.

DBE MOBILE DEVICE SECURITY RECOMMENDATIONS

The emerging mobile environment has the potential to develop new mobile apps and technologies that will enhance the mission of various Federal agencies, their employees, and DBE contractors. The mobile device guidelines published by NIST in 2013 embrace the need for innovation in leveraging the unique capabilities of mobile devices, while also recognizing the accompanying potential for new types of breaches of security and privacy [16]. The results of this survey demonstrate that the current approach is insufficient. However, until the U.S. DOT takes care of its own security weaknesses and takes a leadership role to support the DBEs under Federal contracts to improve their mobile device security, we recommend that DBEs should adopt the following list of security practices.

1. **Subscribe to a mobile device management (MDM) system**. For DBEs with an in-house IT staff, in-house management of the MDM is an option. For smaller DBEs or those that do not want to manage the MDM system in-house, there are many 3rd party vendors that provide MDM services for a monthly fee. At a minimum, the MDM should ensure the installation and updating of antivirus (where appropriate), data wipe, strong access authentication, VPN usage over Wi-Fi, and software updates prompts, and the MDM should forbid jailbroken or rooted devices. Other popular features to consider include data loss prevention, encryption, and application blacklisting/whitelisting. If the DBE decides not to deploy an MDM, then it should follow the minimum recommendations listed below.
2. **Purchase a dual persona device or software**. A dual persona device can separate the business environment from the personal environment. If possible, use a MDM system with the business environment and follow the basic security rec-

ommendations, given below, for the personal environment.

- Prohibit installing or using social media and other applications, especially free applications, in the business environment. A dual persona device will allow for such applications to be installed in the personal environment, while protecting the business environment.
- Do not download and install applications from untrusted 3rd party markets.

3. **Establish basic mobile device security policies**. If the DBE decides not to deploy MDM, then it should establish these policies for its mobile device use.
    - When appropriate for the device, install a security suite that includes antivirus software, data wipe, backup, secure Web browsing, and GPS location and lock,
    - Avoid jailbreaking or rooting the device,
    - Create a complex access mechanism, such as a personal password or passphrase,
    - Prevent applications from storing credentials,
    - Avoid applications that ask for excessive permissions, such as reading your contact list,
    - Keep applications and operating systems updated, and
    - Use a VPN over Wi-Fi networks in public places.
4. **Purchase a new device as necessary to keep the operating system from getting too outdated.** For example, if an Android device's operating system is not 4.2 or newer, purchase a new device. Android 4.4 or later is preferable for new devices. If an iOS device has an operating system older than version 6, purchase a new device. Apple's iOS 7 or later is preferable for iOS devices.

The ideal solution for DBEs is to include a MDM system on a dual persona device and minimize non-pertinent applications in the business environment. The MDM protects the business environment and it remains separated from the personal environment, where more risky applications reside. The second best option is a dual persona device without MDM, which maintains separate personal and business environments with basic security precautions for each. The third best option is a business-issued single environment device. However, if BYOD devices are allowed, then a single environment device with both personal data and business data should include all basic security recommendations, and social media and non-business applications should be eliminated. The least good option, but perhaps the most common, is a single environment device with both personal and business data, social media applications, and other downloaded and installed applications. DBEs, in this situation, should follow the minimum basic security recommendations: purchase newer devices or upgrade to a newer operating system for added protection. The U.S. DOT should also begin implementing the NIST mobile device guidelines and provide support to DBEs to minimize risk of sensitive government data.

CONCLUSION

Over 1000 Disadvantaged Business Enterprises (DBEs) responded to a survey that gauged their use of mobile devices for business purposes and their ability to secure those devices. A significant finding of this research is that most DBEs used mobile devices for business purposes, but security for these devices was poor. Many respondents failed to adequately address mobile device security by using even the most basic security mechanisms, such as installing antivirus software and access authentication. Many also stored usernames and passwords within applications and used Wi-Fi networks in public places without a VPN. Others downloaded applications from 3rd party markets and jailbroke or rooted their devices. It is a combination of these security blunders that results in the use of the most at-risk devices. Overall, the surveyed DBEs poorly secured their mobile devices and are at great risk for malware.

Since most DBEs used their mobile devices for business purposes; DBEs are contractors supporting Federally-funded U.S. DOT projects; and DBEs also obtain external contracts; it is essential that these businesses protect their business data on mobile devices. The recent audit report of the U.S. DOT demonstrated the U.S. DOT systems have inadequate security, so insecure DBE mobile devices can potentially give hackers, whether harmless or malicious, a path to insecure government systems, including the U. S. aviation systems.

As small and medium-sized enterprises, DBEs also have an important motivation to safeguard their own business survival. The potential risk that their own business, customer, and employee data may be compromised could result in major loss of business and recovery costs, even leading to bankruptcy. Adding the increased risk to DBEs because they are also dealing with Federal data and information systems further magnifies the importance of

DBEs taking the responsibility to manage their own mobile device security. It is our intent that this paper creates an awareness of existing DBE mobile device security problems and lends itself as a basic guide for DBEs to take mobile device security into their own hands.

REFERENCES

[1] Apple. "iOS 8," http://www.apple.com/ios/?cid=wwa-us-kwg-features-com, September 2014.

[2] Apple. "Apple Developer Support," https://developer.apple.com/support/appstore/, October 2014.

[3] Appthority. "App Reputation Report," https://www.appthority.com/resources/app-reputation-report, June 2014.

[4] Cisco. "Cisco 2014 Annual Security Report," http://www.cisco.com/web/offers/lp/2014-annual-security-report/index.html?keycode=000350063, June 2014.

[5] e-CFR. "Security Requirements for Unclassified Information Technology Resources," *Code of Federal Regulations*, http://www.ecfr.gov/cgi-bin/retrievedECFR?gp=1&SID=33b7ab11fb72017ef183b26b893, April 2013.

[6] Eddy, M. "Exclusive: Google Play and Amazon Not Safest Android App Stores," http://securitywatch.pcmag.com/mobile-security/306885-exclusive-google-play-and-amazon-not-safest-android-app-stores, January 2013.

[7] Gartner. "Gartner Says Annual Smartphone Sales Surpassed Sales of Feature Phones for the First Time in 2013," http://www.gartner.com/newsroom/id/2665715, June 2014.

[8] Gartner. "Gartner Says Worldwide Traditional PC, Tablet, Ultramobile, and Mobile Phone Shipments on Pace to Grow 7.6 Percent in 2014," http://www.gartner.com/newsroom/id/2645115, June 2014.

[9] Google. "Google Developer Dashboards," https://developer.android.com/about/dashboards/index.html?utm_source=ausdroid.net, October 2014.

[10] Harris, M., and Patten, K. "Mobile Device Security Considerations for Small and Medium-sized Enterprise Business Mobility," *Information Management & Computer Security*, Volume 22, Number 1, 2014.

[11] IBM. "IBM X-Force: Ahead of the Threat – Overview," http://www-03.ibm.com/security/xforce/, June 2014.

[12] Juniper White Paper. "Juniper Networks Mobile Threat Center Third Annual Mobile Threats Report: March 2012 through March 2013," http://www.juniper.net/us/en/local/pdf/additional-resources/3rd-jnpr-mobile-threats-report-exec-summary.pdf. December 2013.

[13] Knox, M. "WiFi in a PCI World," *Computer Fraud & Security*, Volume 12, 2013, pp.5-8.

[14] Malenkovich, S. "Rooting and Jailbreaking: What Can They Do and How Do They Affect Security?" http://blog.kaspersky.com/rooting-and-jailbreaking/, May 2013.

[15] Mearian, L. "Mobile Malware, Mainly Aimed at Android Devices, Jumps 614% in a Year", http://www.computerworld.com/s/article/9240772/Mobile_malware_mainly_aimed_at_Android_devices_jumps_614_in_a_year, July 2013.

[16] NIST. "NIST Special Publication 800-124 Revision 1: Guidelines for Managing the Security of Mobile Devices in the Enterprise," http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf., June 2014.

[17] OIG. Improvements to DOT's Governance Processes Are Needed to Enhance Oversight of Major IT Investments. *Report Number ZA-2013-057*, Office of Inspector General, U.S. Department of Transportation, March 2013.

[18] OMB. Management of Federal Information Resources. *Circular A-130*, Office of Management and Budget, The White House, November 2000.

[19] Passerini, K., El Tarabishy, A., and Patten, K., *Information Technology for Small Business: Managing the Digital Enterprise*, Springer, New York, New York, 2012.

[20] Redman, P., Girard, J., CosGrove, T., and Bosso, M. "Magic Quadrant for Mobile Device Management Software," http://www.gartner.com/technology/core/home.jsp, May 2013.

[21] Roettgers, J. "Google I/O Statshot: 900 Million Android Devices Activated," http://gigaom.com/2013/05/15/google-io-statshot-900-million-android-devices-activated/, May 2013.

[22] Rubens, P. "Mobile Device Management (MDM) Platform Buying Guide," http://www.enterprisenetworkingplanet.com/netsecur/mobile-device-management-mdm-buying-guide-1.html, August 2012.

[23] Skidmore, S. "What Is Dual Persona Mobile Application Management?" http://www.apperian.com/dual-persona-mobile-application-management/, April 2013.

[24] Spence, E. “Android 4.4 KitKat Continues to Reduce Fragmentation of the Platform Thanks to Google Play,” http://www.forbes.com/sites/ewanspence/2013/11/01/android-4-4-kitkat-continues-to-reduce-fragmentation-of-the-platform-thanks-to-google-play/, November 2013.

[25] Statcounter. “Statcounter Global Stats,” http://gs.statcounter.com/#mobile+tablet-os-ww-monthly-201305-201405, June 2014.

[26] U.S. Department of Transportation. “Disadvantaged Business Enterprise Program,” http://www.dot.gov/osdbu/disadvantaged-business-enterprise, January 2013.

[27] Victor, H. “Android’s Google Play Beats App Store with over 1 Million Apps, Now Officially the Largest,” http://www.phonearena.com/news/Androids-Google-Play-beats-App-Store-with-over-1-million-apps-now-officially-largest_id45680android’s, July 2013.

[28] Wetherly, P. and Otter, D. *The Business Environment:Themes and Issues in a Globalizing World*, Oxford University Press, UK, 2014.

AUTHOR BIOGRAPHIES

Mark A. Harris is an assistant professor in the Integrated Information Technology Department at the University of South Carolina, Columbia SC. He has a Ph.D. in Information Systems from Virginia Commonwealth University and a M.S. in E-commerce and B.S. in Information Technology from Old Dominion University. His research interests include security policy management, awareness training, human factors of security, health IT security, and mobile device security. He has authored multiple papers in well-respected refereed information systems journals and conferences. Before academia, Mark was a senior network engineer for a large university, where he oversaw an extensive computer network.

Karen P. Patten is an assistant professor in the Integrated Information Technology Department at the University of South Carolina, Columbia SC. She has a B.S. in Honors Economics from Purdue University, a M.S. in Civil Engineering from the University of Minnesota, and a Ph.D. in Information Systems from the New Jersey Institute of Technology. Her research interests include agile and flexible IT management, small business mobile telecommunications management, and IT curriculum development. She is the author / co-author of two books and has published articles in multiple refereed journals and conference proceedings. Prior to her academic career, Dr. Patten was a Member of Technical Staff (MTS) and managed emerging information technology implementations at AT&T Bell Laboratories.