[redacted]

[redacted]

[redacted]

Dr. Wibowo

MIS

11-17-2014

Outline

I. Business security smartphone

   a. Common Business Data security methods for Smartphones
      i. Discussing why data security is so important at the business level
      ii. Best Practices and Policies for securing smartphones
      iii. Potential impact on business without proper security

   b. Popular Vendors and the security they provide
      i. ESET
      ii. AirWatch
      iii. SAP

   c. Properly selecting Vendors for your business needs
      i. Research the vendors
      ii. Possible costs incurred to your business
      iii. Selection of the proper vendor

II. Security Aspects of Protecting your Smartphone
   a. Basic Smart Phone Security
      i. Always know where your phone is
         1. Don't leave your phone unwatched
         2. Wireless proximity alarm system
      ii. Use Lock Screen
         1. Face recognition
         2. Voice recognition
         3. Password
         4. Pattern
         5. Pin
      iii. Encrypt Sensitive Info
         1. Confidential business data
         2. Private individual data
         3. Personal Health data
         4. Financial data
   b. Risks of modifying smartphones
      i. Jail breaking

1. Jail breaking is the process of removing the limitations put in place by a device's manufacturer.
2. Is generally performed on Apple iOS devices, such as the iPhone or iPad.
3. Removes the restrictions Apple puts in place, allowing you to install third-party software from outside the app store

ii. Rooting
1. Rooting is the process of gaining "root access" to a device
2. After rooting, you can grant specific applications access to root permissions, allowing them to do almost anything they want to the operating system.

iii. Unlocking
1. Android is an open-source operating system, so anyone can take the Android Source code and create there own version of it.
2. Unlocking a boot loader can theoretically allow you to install non-Android operating systems.

III. Prevention of Data Theft
- a. Be vigilant and cautious with spam messages
  - i. Know what forms they take
    1. Text
    2. Email
    3. Advertisements
- b. Use a Lock Screen
  - i. Use a pin that only you know
- c. Download a known security app
  - i. Apps that can track location
  - ii. Report possible viruses or data breach
  - iii. Remote whip in case of lost or stolen phone
  - iv. Ex. Lookout
- d. Before installing apps read reviews
  - i. Buy or download only from known vendors who have a good reputation
  - ii. Read multiple reviews to ensure the product is genuine
- e. After downloading applications read "permissions"
  - i. Understand what the product is gaining access too and for what reason
  - ii. Any questionable activity should be a red flag pertaining to the product
- f. Reset or wipe phone if trading in or selling
  - i. This will ensure personal information will be removed

Data Security on Mobile systems

Data security is a big concern throughout the world. For example, countries like China have developed their own security networks to deter hackers. Some of the security systems they utilize are Wireless Transport Layer Security (WTLS), Public-key infrastructure (PKI), certificate authority (CA), wired equivalent privacy (WEP), device independent smart cards, and wireless biometric services. These systems protect the Chinese citizen's transactions, verify that messages are safe, plus encrypting and decrypting of messages. The consumer isn't aware of security issues and most businesses sell the smart phones without security plans.

Hackers are now switching their attention to smartphones from PC's. A common malware that is spreading throughout Android phones in China is Geinimi. It is spread through SMS messages. SMS spam is also a concern in many countries. It sends your information to commercial advertising and phishing links. Most users feel Google App's is free from malware it is not. There are growing security concerns throughout the world where these app's can enable hackers to get control of the device. Unfortunately this lack of trust is leading to piracy of apps by the consumers and putting their personal information at high risk. A few more common threats that occur globally to smartphone security are sniffing, pharming, data leakage, and exhausting. Sniffing is a way of tapping or eaves dropping the phone. Pharming is a redirect of web traffic to a malicious site. Data leakage is a transfer of data caused by a virus. Exhaustion is an attack of the smartphones battery draining the power. These are just a few examples of common security threats that are encountered in many countries throughout the world.

Data is not only valuable to its owners, but also others, more specifically hackers. Hackers may be able to gain access to someone's mobile phone, "with malicious software that deletes personal data or runs up a victim's phone bill by making toll calls"(Leavitt). In order to combat the theft of data, many companies and even in some cases the government, have released recommendations as to how to prevent this issue. Data theft prevention in our everyday lives is a constant concern. Everyday the media covers new stories relating to retailers, large organizations and even government databases, your information could be next. Passwords, security applications and being vigilant when

clicking links, are some steps any user can take to minimize the theft of personal information. According to the National Institute of Standards and Technology, "in order for maintaining the security of a handheld device, it involves the active participation of the user"(Jansen). Users have many areas of security prevention techniques to utilize, from additions of security passwords, security malware software, GPS tracking, and data backup, among others. When used correctly these techniques will not only secure a users information, but also prevent it from easily falling into the wrong hand. This research will conclude vital ways users can and should be using to prevent the theft of data from mobile devices.

Smartphones have become an important part of our everyday personal and business life. Our Smartphones contain very important and personal information. It is extremely important that we protect our Smartphones so that we deter individuals from accessing and stealing this information. Not having some form of security on our Smartphone is like leaving our car doors unlocked with valuables inside the vehicle. Individuals can get our information if they hack into our phone, if we lose our phone, or if someone knows is password so it is very important that everyone protect their information. One way to protect our information on our Smartphone is by encryption. Encryption is a reversible process that scrambles your information to look like gibberish so that no one can understand it. You can use encryption to protect any information on your Smartphone such as pictures, text messages, social security numbers, credit card numbers, and phone numbers to name a few. Some Smartphones come with an encryption application built into the hardware and some don't have an encryption application built into the hardware. For those Smartphones that don't have an application built into the hardware, there are plenty of third-party applications to choose from to download an encryption application onto your phone. The prices of using a third-party application to encrypt your Smartphone vary depending on which application and company you use. This technology is something that is evolving and improving constantly so it is important to stay up to date with the latest information so that you can make the best choose for you to which application you should use. Encryption can also be used between individuals that want to exchange information with each other. The individuals involved with exchanging information just have to have the same encryption

application so if they choose to protect and encrypt the information that they are sending between each other then they can do so very easily. Encryption is an excellent way to protect our information and is something we should all do.

When a business has many android smartphones being used by its employees it is important to use some important guidelines for protecting those devices. There should be policies in place directed by the Information technology (IT) department involving some of these practices. An example of one of these policies may be that smartphone users set strong passwords on their phones. Another example would be to immediately report any lost or stolen smartphones directly to IT.

Many companies are using the following best practices. First, a company should establish Secured Socket Layer (SSL) Virtual Private Network (VPN) access to its corporate resources. This would provide encrypted web access to network resources and would minimize demand on IT. Using firewall technology and forming a clean VPN would provide secure data and malware protection for the corporate network. A company should also set different access levels based on device. Different levels of trust should be granted to connections. This will limit user's access to sensitive data and reduce data leakage. Another best practice would be to comprehensively scan all smartphone traffic. A comprehensive scan can be done using a firewall to monitor Wi-Fi traffic or going into or out SSL VPN to guard against malicious malware, Trojans or viruses. Controlling the movement of data while it is traveling is key. IT should be able to scan all this data for malware or outbound botnet attacks which would ruin a corporation's image. Smartphone wireless security should also be up to date to have the capability of running deep packet inspections to prevent virus and spyware. A final best practice would be bandwidth monitoring and activity. It is important to have good service for your employees it could cost you a client. Imagine if you are in the field working with a client and your smartphone service is lost. You may lose the client or a sale based on the fact the client may deem you unreliable

Now that we've discussed some important policies and practices I thought we could talk about a few companies that offer software solutions to protect businesses. There are many companies that are available to help your business with protecting smart phones. We are just going to focus on a few in regards to making their employees phones secure.

These companies not only protect businesses but also the different areas of the government. They offer solutions in many areas. A company like ESET who has been in business for twenty five years offer protection for large and small business and personal software solutions. One of the business products they offer is Endpoint security specifically for Android phones. This product protects your business from malware infections, offers call blocking, and filters spam to minimize data loss risk. Remote administrator management is also offered and this is the ability to monitor and track all of the employee's smart phones. Some of the key benefits with this software are low costs to implement, remote installations and updates, remote anti-virus scanning, active directory synchronization across the organization, enhanced data security, and delayed software updates. The android software also offers frequent and flexible reports which are sent to the remote administrator to alert your company that top clients need spam removed. Security audit for each phone is also included which will check the status of all vital phone functions such as disk space, and running processes. This software is compatible with all android smartphone devices with a version of 2.0 Many industries can use this software whether it is for healthcare, financial, or any government.

Airwatch also has many clients that seek android security. Airwatch mobile security management ensures users, devices, applications, content, data, and networks are secure. The compliance engine for Airwatch constantly monitors devices and escalates actions if non-compliant. These escalation actions are preconfigured and bring devices into automatic compliance. Airwatch VPN ON Demand and APP tunnel work with compliance to grant access to users. Using their own specific Secure Content Locker (SCL), Airwatch can create according to the company's requirements. The mobile workspace software is also a single sign-on that is encrypted and allows compliance monitoring and management. It enables a dual persona to compartmentalize and utilize data without having to manage the device. Basically it means there is a separation between workspace applications and personal applications.

SAP provides many services but is also a vendor of mobile security solutions for companies. They also provide core security functions at the source, transmission and network, and at the device. One of the things that made SAP stand out they encourage companies to assess their current level of corporate security. It helps get a feel for what

they might be lacking from current provider. SAP has the company fill out a questionnaire graded on a point scale. If the company feels their mobile security falls below a certain point scale then it is possible the company may need to make improvements. SAP is hoping one of those improvements is using them to provide Mobile Device Management. These were just a few examples of companies that can aid different industries in mobile device security. As an employer it is very important to do the research and find a vendor that can reduce costs and continue to keep your business running seamless.

There are some simple and basic practices that everyone can do when it comes to protecting your smartphone. The most basic practice would be to not let your smartphone out of your sight. Even letting your smartphone out of your sight for thirty seconds or more jeopardizes your information and puts your phone at risk of getting stolen. A personal story, one day my friend and I were at the gym and my friend placed his smartphone on the bench while we went to get a drink of water out of the water fountain. When we came back his phone was gone and someone was looking at his personal information. The walk to the water fountain and back might have taken a total of sixty seconds and in that time someone took his phone and began accessing his personal information. That is why it is so important to keep your phone on you or within your eyesight at all times. Think of your phone as a money clip with one thousand dollars in it, because it will help you to never let your phone out of your sight for a single second. Another simple thing that everyone can do to protect their smartphone and all of their sensitive information that is in it is to use a screen lock. In order to have a screen lock all that someone has to do is go to his or her settings menu and activate it. A person doesn't have to download anything or purchase anything. There are a number of different locks for a person to choose from such as using a pin number, a pattern, or a password. When selecting a screen lock a person should choose something that is hard for others to figure out. For example, using a person's birth year as a four-digit pass number or using the word password, as a password is easy for someone to figure out. If someone is going to use a pin number it should be an eight-digit number with a mix of multiple numbers in it. If someone is going to use a password it should be a mix of upper, lower case letters, and symbols. I personally recommend that a person use a mix of both numbers, upper case

letters, lower case letters, and symbols if they are going to use the password/pin option. Downloading or purchasing an application that uses face recognition or voice recognition is another option that a person has to screen lock their phone. If this is the option that someone wants to choose they should look into which application is compatible to their phone and select the best option for them.

Using encryption is also a simple way to protect your smartphone. Encryption is basically the scrabbling or disguising of information in your phone so that a person cannot tell what the information says or what things look like. Encryption is like creating a mirage or hiding your valuables in your home so even if someone got through your locked front door all your valuables would be hidden and not visible to take. In order for someone to be able to read the information or be able to look at it in its original form they would need a key that would only be given to a person with the same decryption application and linked to their contact or friend. Certain phones have encryption options built into the phone that they can use. There are also several services and applications that a person can purchase or download to encrypt data. The main thing is that a person needs to use the same encryption service as their friends or contacts because having the same is necessary in order to be able to decrypt the information and view it. Information that a person should consider encrypting would be confidential business data, personal data, personal health data, and financial data.

When it comes to protecting your smartphone a person needs to understand the risks of modifying their phone. Jail breaking, rooting, and unlocking are three popular ways that a person can modify their phone. Smartphones include a layer of Digital Rights Management (DRM) software, which exists to limit the software you can run on it or is there for security reasons. Jail breaking is the process of hacking these devices to bypass DRM restrictions, allowing you to run software that is not approved and other tweaks to your operating system. This opens up the door to malware and hackers to easily access a user's data. Jail breaking this typically done on the iPhone or iPad. Rooting is the process of allowing users of a smartphone to attain privileged control or gain root access within a sub system. With a rooted phone a person can run applications that require access to certain system settings. Since root access circumvents the security restrictions that are put in place, there is not really any effective way to tell just what the application

intends to do with that power. There have been stories where people who have rooted their phone have had their Gmail application replaced with a modified version, had files deleted, gain access to a person's market account and make purchases on their behalf, and many other horrifying stories. Rooting is typically done on an Android phone. Unlocking is when your cell phone can be used with more than one wireless carrier, for example it can be used with AT&T and T-Mobile. Wireless carriers did not want to pay for a phone and later have it used with another carrier, so they got the cell phone manufactures to design the phone to be locked to just their service. Unlocking can be done with any phone and different carriers can be used together such as T-Mobile and AT&T and Verizon and sprint can be used together. If someone unlocks an Android phone, which is an open-source operating system, it opens the possibility that it can be accessed and a hacker can create his or her own version of it. It is important to know that all three modifications jail breaking, rooting, and unlocking all lower the security of a person's phone and put a person's information at risk of being hacked.

Data theft has boomed over the past years, and it can be attribute many different aspects of mobile security. According to a report posted by a computer-networking firm known as Juniper Networks Mobile Threat Centre, it was stated that, "mobile malware threats grew at a rate of 614% from March 2012 to March 2013" (Karena 2014). Scarcely a week goes by that the media doesn't cover another major leak of data that includes personal information, private photographs, or even corporate secrets. Hackers can gain access to information in a number of ways, but there are also many strategies an individual can use to prevent this from happening.

First is simply to be vigilant. Lacoon Mobile Security advises all mobile users that "you need to be vigilant about what you download onto your mobile device. It is important to understand what each and every app is going to do, including ours!" (Mobile Device Security 2014) Learning and understanding different ways hackers gain access to a mobile device can become a major life savor. Access can be gained to a mobile device in a number of ways. These may include malicious text messages, emails, fake advertisements and applications embedded with malware. By clicking on a link sent through any of these gateways, or downloading a malicious app, may allow access to the

mobile device. Taking simple steps such as only accepting and reading messages from known sources and/or avoiding clicking on advertisements that "are too good to be true" can further secure a mobile device. Also, when downloading applications, know if the developer is reputable. Doing some quick research on the developer or the application, can allow some easy insight into the application and if it is safe or not. Downloading applications from well-known or reputable developers helps ensure that applications will be safe. If an application is not from a known developer, reading multiple reviews from different sites will aid in knowing whether or not to use the application.

Another simple, but valuable way to secure a mobile device is the use of a lock Screen. The simple "PIN" or design lock screen can drastically increase the security of your device if it was ever stolen. Software developers have even taken it a step further in recent years and added features such as fingerprint identification, picture authorization and voice recognition. By using this security, it can help ensure that if a phone falls into the wrong hands, it will be difficult to impossible for someone to gain access to the data preserved on the phone.

As mobile phones become more advanced, they often contain personal and business information. Like personal computers, mobile devices also need protection as well. Due to the compact size of the mobile phone, it becomes easier for gain access to and misplace. A great way to ensure the security of a mobile device is the instillation of security software. Many developers have released different security programs such as "Lookout" and "Lacoon" Mobile Security, which have advance features such as cloud back up services, application monitoring, GPS monitoring, and reset/wipe features. These features that security programs offer can become critical in the prevention of data theft. While most phones come with basic security features, "it may be enough to deter your friends or mother from looking at your information," but this basic security is not enough "to protect your phone from viruses or knowledgeable hackers" (Mobile Security Software Review 2014). Cloud back up services allow users to back up any information (text and phone call information, photos, application data, contacts etc…) into a cloud data base that can be retrieved from either another authorized mobile device or computer. Application monitoring aids in the identification of viruses and malware, that is attempting to gain access through new applications or downloaded content. By

monitoring the content being installed on the mobile device, the security can identify code that is malicious and deny access to the users personal data. GPS monitoring is also available and becomes quite useful. When the device becomes lost or stolen, users can turn on the GPS location through another computer and track or find the device. If all else fails, users can use the wipe feature and remotely wipe all content to ensure sensitive information does not fall into the wrong hands. By utilizing the software offered by security applications, users can help ensure that data stored on their device is secure and in the case that the mobile device falls into the wrong hands it can remotely tracked or wipe to ensure maximum security.

Lastly, users who download applications should be cautious as to what the application is requesting access to. When an application is downloaded it will request access to a variety of features and reading the "permissions" page will ensure the user understands what the program is doing. Programs gaining access to features such as the GPS location, should be questionable and further looked into if the application primary use does not need access to the type of feature. If users notice questionable activity pertaining to the permissions access of a product, should further research the application or contact the developer for further explanation.

If users take the necessary precautions to ensure the security of their information, they will be able to enjoy their mobile device without concern for personal information leaking to an unintended user. Users who are vigilant, use security features such as lock screens, download reputable security application, read application review pertaining to the product and being vigilant to what applications are gaining access too, will ensure that data will remain safe on the device and prevent hackers or other users from taking personal or business related content.

In conclusion, our research has found a number of areas where the security of mobile smartphones is in jeopardy of being compromised. First the business aspect of smartphones has a number of areas that need great attention, in order to have the best possible outcome for security of mobile devices. Common business security methods such as best practices and polices as well as understanding the potential impact on business if proper security is not met is critical. Proper vender selection is also key in

order to obtain the best possible security. By properly researching vendors, the cost that may be incurred, and the selection is crucial to proper business security. Second, the basic aspects of smartphone security will help individuals on a personal level. Always knowing where your phone is, using integrated security features, encrypting sensitive information, and knowing and understanding the risks of modifying smartphones will enable the user to maintain the best security and protecting there information. Lastly, the prevention of data theft by being vigilant and cautious with spam messages, downloading a known security application, reading application reviews before instillation, and read the permission to which a phone needs access to will allow the user to properly secure their information and prevent data theft.

References:

"Android Security." *Android Security*. ESET. Web. 9 Nov. 2014. <http://www.eset.com/us/business/products/security-android/>.

Barrera, John Fredy, Alejandro Mira, and Roberto Torroba. "Optical encryption and QR codes: secure and noise-free information retrieval." Optics express 21.5 (2013): 5373-5378.

"Containerization." *Airwatch*. Airwatch. Web. 9 Nov. 2014. <http://www.air-watch.com/solutions/containerization>.

Chao, Hong, et al. "To Root or Not to Root? The Economics of Jailbreak." The Economics of Jailbreak (June 5, 2013) (2013).

Dubois, Renaud, Aurore Guillevic, and Marine Sengelin Le Breton. "Improved broadcast encryption scheme with constant-size ciphertext." Pairing-Based Cryptography–Pairing 2012. Springer Berlin Heidelberg, 2013. 196-202.

Enck, William. "Defending users against smartphone apps: Techniques and future directions." Information Systems Security. Springer Berlin Heidelberg, 2011. 49-70.

Govindaraj, Jayaprakash, et al. "Poster: iSecureRing: Forensic ready Secure iOS apps for jailbroken iPhones."

Karena, Cynthia. "How to Stop Your Smartphone from Getting Hacked." *The Sydney Morning Herald*. N.p., n.d. Web. 02 Nov. 2014.

Leavitt, N. "Mobile Phones: The next Frontier for Hackers?" *IEEE Xplore*. N.p., n.d. Web. 09 Oct. 2014.

"Mobile Device Security | User Privacy FAQ - Lacoon." *Lacoon Mobile Security*. N.p., n.d. Web. 02 Nov. 2014.

"Mobile Security." *Airwatch*. Airwatch. Web. 9 Nov. 2014. <http://www.air-watch.com/solutions/mobile-security>.

"Mobile Security Software Review 2014 | Best Mobile Security Apps - TopTenREVIEWS." *TopTenREVIEWS*. N.p., n.d. Web. 02 Nov. 2014.

"Remote Administrator." *Remote Administrator*. ESET. Web. 9 Nov. 2014. <http://www.eset.com/us/business/products/remote-administrator/>.

Schrittwieser, Sebastian, et al. "Guess Who's Texting You? Evaluating the Security of Smartphone Messaging Applications." NDSS. 2012.

"Software Solutions." *Software Solutions and Device Management*. SAP. Web. 9 Nov. 2014. <http://www.sap.com/pc/tech/mobile/software/solutions/device-management/security.html>.

Jansen, Wayne. "Guidelines on Cell Phone and PDA Security." *Guidelines on Cell Phone and PDA Security* (n.d.): n. pag. *National Institute of Standards and Technology*. U.S. Department of Commerce. Web.