Managing Application Security of Mobile Devices:

Bring Your Own Device

Michelle Rowton

Table of Contents

Abstract

Mobile device management is an important topic for companies considering the use of a mobile device policy. There are several vulnerabilities that can be caused from outside sources, not to mention vulnerabilities that come from the inside. McAfee, a leader in antivirus is reporting that the top cyber threats for 2014 are attacks on mobile devices (Gormisky, n.d.). A mobile device that has been attacked can compromise corporate data. Companies need to do the research involved in securing mobile devices before accepting the possibility of "bring your own device" to the workplace.

For the purposes of this paper I intend to point out the problems in the security of mobile devices. I will cover several of the policies a company might need to be involved in "bring your own device" in the workplace, followed by what employers are doing or need to do to ensure the safety of their information.

Managing Application Security of Mobile Devices:

Bring Your Own Device

With application security being such a hot topic in the technology world these days as well as in courtrooms, companies need to ensure there isn't any sensitive data being leaked to the public or being stolen by hackers. It's hard enough to keep data secure within the confines of the company doors, but mobile devices are just that, they are mobile. The IT Department can't follow people around with their device so there needs to be something to help the devices to be managed from another location.

Because it's hard to secure mobile devices, this is a huge security concern for most companies, but when companies need to secure mobile devices that are brought in by the users it can bring a whole new realm of problems. Most users don't understand the importance of securing their devices even if they do have company information on them. Especially when they feel it's a breach of their rights when they are using their own phone, they should get to do what they want with it and when. This is not the case. Company data belongs to the company, even if it resides on someone else's device, therefore if the company wants this data secure, they need to take the steps to do so. Just because the device functions the way it should does not mean it follows the needs of the CIA triad.

It is important to consider the options in managing mobile devices as it pertains to bringing your own device to the workplace, so we will make sure to cover this topic. From this point forward we will use the acronym BYOD which stands for Bring Your Own Device.

Literature Review

EY (2013) states that estimates suggest that in only about 5 years the number of mobile devices will be up to about 10 billion. That's 1.5 mobile devices for every person on the planet! That's a lot of mobile devices! The use of mobile devices is only increasing and the use of mobile devices in the workplace is just as common these days as using the front door to walk into the workplace. The more popular mobile devices become, the more likely they are to be subject to attack.

Review of Risks

When considering BYOD in the workplace, it's always important to assess the risks involved. In an article by Milligan and Hutcheson (2008) they compiled a list of mobile device security problems/risks and went so far as to even suggest countermeasures that can be performed in an attempt to mitigate such risks. The following were listed by Milligan and Hutcheson (2008) as the most common risks of using mobile devices:

- Viruses, worms or other PDA-specific malware – this is a problem that can be created by opening email attachments that contain a virus or worm. This can be minimized by being cautious of what you click on in emails.
- Theft of sensitive data – stolen or lost devices are at greater risk. Securing a device with a password, making sure your device is not discoverable on Bluetooth, and using encryption should help to minimize this risk.
- Exposure of critical information through wireless sniffers. Wireless intruders could capture e-mails, e-mail addresses and attached data if security is insufficient. – Again, making sure to use encryption on a device can prevent the exposure of critical data.

- Loss, theft or damage of device – This can be prevented with a little extra physical security. In the event a device is stolen or lost, it may be important to know how to remotely wipe a device to prevent theft of data.
- Use of the PDA as proxy to establish a virtual connection from an attacker to an internal network
- Data loss/leakage due to the small footprint and portability
- Fraud enabled by remote access or copying mass amounts of sensitive data – This is a problem that stems from a disgruntled type of employee. This is one of the most difficult risks to prevent. The only real way to prevent this is to know the signs and to watch for irregularities in network traffic and/or irregular amounts of downloads.
- Spam causing disruption and driving up service costs if targeted toward mobile devices
- Malformed Short Message Service (SMS) messages causing devices to crash

EY (2013) finds that often the risks between BYOD and the current network to be very similar and divides the risk landscape into three important areas:

1. Securing mobile devices
2. Addressing application risk
3. Managing the mobile environment

Review of BYOD

Citrix (2013) defines BYOD as "any strategy that allows people to use their own devices, whether occasionally, primarily or exclusively, for work." There is a lot of data out there for discussions on whether employers should allow or disallow the use of BYOD in the workplace.

Whether it's a corporate owned device or an employee owned device there are still risks that need to be considered, but there are also many benefits to the use of a BYOD policy; including increasing the productivity in the workplace. Citrix (2013) lists some of the benefits of BYOD as follows:

- Empower people to choose their own devices to improve productivity, collaboration and mobility
- Protect sensitive information from loss and theft while addressing privacy, compliance and risk management mandates
- Reduce costs and simplify management through self-service provisioning and automated management and monitoring
- Simplify IT with a single comprehensive solution to secure data, apps and devices

Citrix (2013) states that the average number of devices currently connecting to a corporate network is 5.18 per knowledge worker and 4.43 devices across all workers. They think this will rise to almost 6 devices by the year 2020.

Like everything else though, BYOD does have its Pros and Cons. Gibson (2014) lists the Pros and Cons to consider with BYOD. The Pros of BYOD are the Technology Budget, Familiarity, 24/7 Learning, Digital Literacy, Reaching Reluctant Learners, and Resources. The Cons of BYOD are the Costs of BYOD, Limitations, Slow Networks, Security, Poverty Gap, and Is Everyone on Board? (Is there full support?).

One concern/problem with BYOD pointed out by Ellis, Saret, and Weed (2012) is that employees still tend to perform some type of unapproved work on their personal device. "Employees expect fewer restrictions to their personal activities, particularly if they are paying for the devices themselves." (Ellis, Saret, and Weed, 2012, p. 7)

Review of Employer Controls

Milligan and Hutcheson (2008) state that the key elements necessary for mobile device security are essentially the same as they have been for the past 20 years of technology security:

- Access control (Mobile devices inherently lack physical access control. They are used in public places where risks of data loss, device loss, probing and downloading data by unauthorized people are the highest.)
- User authentication
- Data encryption
- Intrusion prevention
- Antivirus and antimalware software applications
- Administrative standards and infrastructure
- E-mail security
- Network perimeter and transmission security

In an article by Sophos (n.d.) they recommend the following three priorities for securing data for every organization:

1. Enforce an acceptable use policy
2. Implement strong device security
3. Demonstrate regulatory compliance

Sophos also states that "most data breaches on mobile devices are typically due to basic security failure—weak (or no) passwords, failure to encrypt data, falling victim to phishing or other social engineering, and failure to update the device (making it vulnerable to simple attacks). Getting the basics under control and making sure you can purge devices when they go

missing should be the highest priority, both to minimize actual risk of data loss and to satisfy regulators." This means that they are basically assuming the weakest link is really the operator of the device.

Sophos (n.d.) recommends an acceptable use policy, but there are several other policies that may need to be put into effect if a corporation is considering BYOD. Citrix (2013) recommends several policies, including the following:

- Eligibility
- Allowed devices
- Service availability
- Rollout
- Cost sharing
- Security
- Support and maintenance

These types of policies are fairly standard in most places of employment that have enforced the option of BYOD.

Gaps in Literature

One of the things not mentioned in the literature was the third party applications that can help a corporation to secure their mobile environment and even their network from potential risks. Some of the third party applications that can assist a corporation in mobile device management are Fiberlink MaaS360, XenMobile, Airwatch, and MobileIron.

Most mobile device management systems allow an IT Department to remotely wipe or disable a device and require security passwords on a device. This solves many of the security concerns with mobile devices, especially from lost or stolen phones. Mobile device management can also force the use of antivirus on phones which is starting to become a necessity as more and more malware is focused towards mobile device users.

Another thing I didn't see mentioned as an option for prevention was educating the users. I think if users were more aware of what is actually out there preying on them, they may choose to be more cautious. Some of the biggest risks seem to be things that could be prevented if the user was made aware of how to prevent the attack, such as opening emails from unknown senders. This is where security policies could come in handy as long as the users have access to them and are encouraged to read and follow them. Listed below is a breakdown of a few of the common BYOD policies.

BYOD Policies

The BYOD policy can either be one policy that encompasses all of the policies necessary to secure the mobile devices or it can be broken down into several policies. The benefit to having several policies is that it's easier to manage and update one small portion at a time rather than the entire policy all at once. Below are a few suggested policies that can be used. This is definitely not an exhaustive list.

BYOD Eligibility Policy

This would be a policy listing the topics of eligibility criteria to employees such as roles, titles, and if approval is required. If approval is required, this would also outline the process of getting management approval. Geographic and organizational eligibility would also be outlined,

for instance some positions may require the use of a mobile device and therefore are eligible, while jobs such as the phone operator of a company may not have the need for a mobile device and therefore would be ineligible.

BYOD Allowable Devices Policy

Some companies may have a preference on what devices are allowable under their BYOD policy. Reducing the types of allowable devices down to only a select few can be beneficial to an organization due to the fact that it reduces the types of devices the IT staff will need to have knowledge of. The type of device may be preferred also for security reasons. If a particular device commonly has a security problem, this would cause a company to decide not to support that device. This type of policy would list which types of devices are allowable, which model/brand of devices is allowable, and possibly even which phone carrier the device can use.

BYOD Cost Sharing Policy

This type of policy will outline how much money a company is willing to share towards the bill of the device, such as a phone bill. Some organizations will base this on the rank of the employee within the company, giving more compensation to upper management and higher ranking employees.

BYOD Security Policy

This type of policy would outline device requirements such as passcode requirements, reporting a lost or stolen device, restrictions on applications that could cause vulnerabilities, restricting the use of cameras or Bluetooth devices, and the instructions on how to locate or wipe a lost or stolen device. This may also outline the apps that are required to be downloaded onto the phone such as antivirus software or encryption tools for email.

BYOD Support

This would list the extent of what the company is required to provide support for a device. Most companies will assist with things such as setting up email accounts for the first time or setting up the required applications, but will rarely provide technical support, that is typically done through the phone vendor.

Discussion

EY's (2013) estimates suggesting that in only about 5 years the number of mobile devices will be up to about 10 billion makes it clear that mobile device security is on the rise and needs to be considered as important in the corporate environment. The increase in the use of mobile devices only creates an increase in the ways we are vulnerable to attacks by hackers and data thieves.

Milligan and Hutcheson (2008) did a great job compiling their list of mobile device security problems and risks including countermeasures that can be performed in an attempt to mitigate such risks. This is obviously not an exhaustive list, but it is a great place to start when assessing the vulnerability of your mobile devices.

EY's (2013) technique of dividing the risk landscape into 3 important areas can assist with the management of mobile devices by making it more manageable. Breaking those areas down into their own policies would take the management even one step further towards a secure environment.

Citrix (2013) was able to list some encouraging facts about BYOD that makes BYOD seem like a great idea for corporations. The most encouraging being the increase in productivity that can be noticed within the company with the use of BYOD. As popular as mobile devices

have now become, it would be difficult for most employers not to see the logic behind implementing the policy.

Creating BYOD policies is an important step in the implementation process. Not only do policies help to protect a corporation, they also let employees know what the expectations are of them.

There will always be gaps in literature, so it will always be beneficial for companies to do their own research rather than just rely on the research of others. Also, it will always be best for a company to adapt policies as time goes by. Technologies change constantly and something that isn't a problem currently can turn into a problem later on down the road.

Conclusion

We were able to conclude that there are many vulnerabilities that should scare most corporations into developing an in depth mobile device security policy. The article by Milligan and Hutcheson (2008) was helpful in concluding with some common sense tips that corporations need to consider. First and foremost they need to recognize the risks and commit to taking action on those risks. I think this really sums up the solution to the problem. Acting as if there is no problem, is a problem in itself. Employees will typically find a way to use mobile devices at work whether it is written into the policy or not. Even if employers don't support the BYOD policy, they should consider the security implications involved. Even company owned mobile devices can come with risks. It's clear that the usage of mobile devices is here to stay. Companies would be best suited to follow the crowd and jump on board now, before they set themselves up for a security breech or failure. The use of third party applications and a control of the applications allowed on the mobile devices can assist with this.

References

Milligan, P.M., & Hutcheson, D. (2008). *Business Risks and Security Assessment for Mobile Devices.* Retrieved from http://www.isaca.org/Journal/Past-Issues/2008/Volume-1/Pages/Business-Risks-and-Security-Assessment-for-Mobile-Devices1.aspx

Sophos (n.d.). *Mobile Security 101.* Retrieved from http://www.sophos.com/en-us/security-news-trends/security-hubs/mobile-security/mobile-security-101.aspx

Citrix (2013). *Best Practices to Make BYOD Simple and Secure.* Retrieved from http://www.citrix.com/content/dam/citrix/en_us/documents/oth/byod-best-practices.pdf

EY (2013). *Bring Your Own Device: Security and Risk Considerations for your Mobile Device Program.* Retrieved from http://www.ey.com/Publication/vwLUAssets/EY_-_Bring_your_own_device:_mobile_security_and_risk/$FILE/Bring_your_own_device.pdf

Gibson, K. (2014). *The Pros and Cons of BYOD.* Retrieved from http://www.insight.com/insighton/education/the-pros-and-cons-of-byod/

Ellis, L., Saret, J., & Weed, P. (2012). *BYOD: From Company Issued to Employee Owned Devices.* Retrieved from http://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/high%20tech/pdfs/byod_means_so_long_to_company-issued_devices_march_2012.ashx

Gormisky, L. (n.d.). *Mobile, Cloud, Stealth Attacks Lead Cyber Threats for 2014.* Retrieved from http://partners.decisionbriefs.com/defense-daily/article/mobile-cloud-stealth-attacks-lead-cyber-threats-for-2014-mcafee-says/

MaaS360.com (n.d.). *BYOD Policy Guide.* Retrieved from https://alliance.cisecurity.org/opportunity/documents/BYODPolicyGuidecopy.pdf