Security and Privacy Considerations for BYOD

Carol Woodbury, President

SkyView Partners, Inc

Introduction

The world of BYOD (Bring Your Own Device) is rapidly expanding.   You may not think it's happening in your organization but it's very likely that employees are using personal devices for business purposes. Even if you don't allow the devices to connect directly to your network or to receive an individual's email, it is likely that mobile devices are being used to take notes in meetings, upload and share files, coordinate work and personal calendars, and more. If you don't think this to be the case or you have the belief that this is not occurring in your organization, look around you – you may be shocked at what you see.

To help you determine what stance to take on the use of personal devices within your organization, this white paper discusses the security and privacy considerations you'll want to consider as well as the technology that can be used to secure these devices.

What is BYOD and what's the Issue?

BYOD (Bring Your Own Device) is when someone uses their own mobile device – typically a smart phone or tablet – to perform part or all of their job functions. BYOD is becoming more popular because of the convenience it offers. By consolidating into one smart device, gone are the days of carrying a work-issued phone, a personal phone, a pager and a digital music player. And depending on the employee's job, they may even be able to eliminate carrying a laptop – especially when traveling. In addition, many applications (such as file-sharing and note-taking) available on these devices offer time-savings and convenience. But it's this convenience coupled with the ease in which corporate assets can be accessed, stored and forwarded as well as the co-mingling of personal and corporate data that causes BYOD to be a security and privacy concern.

Why Now?

You may argue that employees have been using their own devices for many years. For example, many users have long used their own PCs to connect via a VPN connection to work from home. So what's the big deal now?

One issue is the **mobility** of the devices. Connections can be made to corporate networks over public, unsecured networks from literally anywhere in the world. Couple this with the fact that these devices are easily **lost or stolen**, as well as other **security issues** with these devices (including the rapidly growing number of malware-infested applications), the threat presented by these devices to your organization is expanding exponentially.

Additional Considerations

The **storage of corporate data** – including data that may be under regulatory compliance requirements - is one issue to consider. Just because data is on a mobile device does not eliminate it from compliance requirements. In fact, some laws (such as the breach notification law for the State of Massachusetts) have requirements that specifically apply to data on mobile devices. Regulated data such as healthcare information, credit card numbers and PII (Personally Identifiable Information) as well as confidential corporate information is most likely being stored unencrypted on a mobile device. In addition, any requirements to log the access or use of this data are not being fulfilled. And any additional access controls enforced on the server where the data is stored have long since been eliminated once the data becomes resident on the mobile device.

Another issue that will likely give you pause is the consideration for where the mobile devices are being backed-up. You must consider where the device – and therefore, your organization's data – is currently **being backed-up**. Most devices are, at the very least, backed up to an employee's home PC or laptop. But many devices are backed-up to cloud-based storage (think iCloud, Google, Microsoft SkyDrives, etc) If the thought of your organization's data being backed-up to general-purpose, unsecured cloud-based services doesn't make you stop and consider the security issues with BYOD, it should.

Also, many organizations have a **data retention policy** that eliminates data after a certain period of time. When information is stored on the mobile device and worse, in a cloud-based back-up, are your data retention policies being followed?

You should also consider what happens when the employee leaves the organization – either voluntarily or via termination. What is going to happen to your organization's data that is currently resident on the employee's mobile device or that's stored in the former employee's cloud storage or back-up repository?

Finally, the incidence of malware on mobile devices is rising rapidly. Many of the viruses and malware come from infected applications which are never reviewed or screened prior to being downloaded to the device. Is your organization prepared to scan for and respond to this threat?

How do You Decide

When deciding your approach to BYOD, there are a number of factors to consider. Let's discuss those now.

What Devices and Who Supports Them

When determining your BYOD approach, you must determine what devices are allowed and who provides the technical support. That is, who's going to provide technical support if the phone fails, can't connect to your network or otherwise doesn't work as expected? The answer to what devices are allowed and who supports them is easy if your organization provides the devices. But what if it's the employee's device?   Do you allow *any* type of device – including any release of the device past or current? And where do you draw the line when it comes to supporting technical issues with the device? Will you provide support even if the issue is not necessarily related to using the device for work-related tasks?

Use of Technology

Most organizations that allow use of BYOD are implementing some form of technology to limit access and secure access to corporate resources. Even if the devices are provided by the organization, the technology available provides additional security layers that many organizations choose to implement. The task of managing and securing mobile devices for enterprise use is one of the most rapidly developing areas of technology today. Let's take a look.

Mobile Device Management (MDM) - MDM is software that allows you to secure, monitor, manage, and support mobile devices deployed across mobile operators, service providers and enterprises.   This technology implements 'containerization' where work-related apps are segregated from personal apps. It also allows you to disable functions such as Copy/Paste between work and personal containers. You may also see this technology referred to as "workspaces" or "sandboxing."

MDM can also be provided by the native operating system itself. One of the benefits of using the native support is that you can preserve the "user experience" of the device. One of the downfalls, however, is if you are providing BYOD and you literally allow any device then you have write to and manage numerous operating system interfaces to manage all of the devices.

Mobile Container Management (MCM) – Rather than managing the entire device, this emerging technology manages only the container associated with the enterprise. With this technology, the mobile device is virtualized. One image (container) houses the user's personal apps and data and the other belongs to the enterprise. Only the enterprise's container is managed. This eliminates some of the employee privacy issues when managing the entire device. (See the discussion of privacy issues later in this paper.) MCM is emerging now because virtualization has recently been made available on mobile devices.

Mobile Application Management (MAM) – MAM is software that allows you to manage applications on both employee-owned and an organization's mobile devices. It can be used to manage the deployment, updating, removal and licensure of applications, provide tracking of what is installed on each device as well as an extra layer of security including authentication, access control and encryption. It stops short of managing the entire device.

The extra layer of security used by MAM is accomplished using a technique called '**app wrapping.**' App wrapping adds an additional binary before the start-up of the application that allows you to require additional authentication, determine where the request is coming from (home network, public network or VPN access, for example) and route the request to the appropriate server or prevent access altogether and determine whether data can be stored on the device. App wrapping can also disable features such as the camera and copy/paste but it would apply to the individual app rather than for the whole container that MDM would restrict.

MAM typically comes with an enterprise app store – a set of apps approved by the enterprise for download and use on the mobile devices.

App Streaming – The principle behind app streaming is that neither the application nor the data actually resides on the device itself. While a rather old concept (think X-Windows), it is a newer and less explored technology in the world of managing and securing mobile devices. The benefit of this technology is that data never actually resides on the mobile device itself, thus eliminating the security issues when a device is lost or stolen and the privacy issues of wiping an employee's personal data.

Because of the rapidly evolving nature of these technologies, the best way to find what is currently available is to do an Internet search using the technology term (e.g., mobile application management) as your search criteria. Look for the most recent articles about the technology to learn about the latest developments.

Providers of the Technology

The providers of this technology are developing as rapidly as the technology itself. At last count there were at least 100 vendors vying for this space, including the mobile device providers themselves. Apple recently announced it's adding MDM technology to iOS 7 to enable enterprises to manage mobile devices, secure applications and use VPN secure connections when accessing enterprise data. It's also providing support for an enterprise app store. In addition, if you look at MDM technology it's conceptually similar to managing users' desktops and corporate issued-PCs. Seeing a shrinking market in their current offerings, the vendors of managed desktop software and services are also getting into the MDM space.

Technology acquisitions by major players in this space are already occurring. Obviously, this is a rapidly evolving arena. When choosing a technology and a vendor to provide the technology, look for one that is updating their product line and services along with the evolving technology. Implementing this technology will not be trivial. You don't want to be committed to a vendor that remains stuck in old technology once new technology is developed.

Privacy Issues

The discussion so far has been centered around the issues of corporate data on an employee's device. However, employees' rights need just as much consideration as the security of corporate data before you determine your position on BYOD. Several situations may violate employees' privacy if you allow BYOD. You need to be aware of these situations and determine how to handle them as part of your BYOD strategy. Above all, employees participating in your BYOD program must be aware of the following:

Use of technology that wipes the device if it's lost or stolen. If the device is wiped, that typically means all data – including personal data. If the personal data isn't being backed-up, it's gone…forever.

Use of technology that tracks the phone's location (so it can be wiped if lost or stolen) is, in effect, tracking the employee's location – even during off-hours. How this information is used and who has access to it must be considered by the organization and communicated to the employee.

Use of technology that keeps an inventory of the apps installed on the device may also inventory an employee's personal apps. Also the use of these apps may be logged. As an organization, you need to decide what and when activity is logged, how this information is used and again, who has access to the information.

e-Discovery: If the device contains data that is part of the e-Discovery process due to litigation against the organization, the phone will be taken from the user. In this case, all activity performed using the phone is open to examination. This includes apps used, personal pictures and email, websites visited, etc. Also, the device may be kept for a lengthy period and the employee will be without the use of their device during that time.

For some employees, the thought of being tracked by their organization or having their personal device wiped will cause them to choose not to participate in a BYOD program; therefore, it's imperative that your employees are fully informed of these issues *prior* to your allowing them to participate in BYOD.

What are your Options?

By now you've probably realized that you need to do something to address the issue of BYOD. So what are your options? Organizations that have recognized that their employees are bringing their own devices are typically implementing some variation of one of the following:

- Allow employees to use their own devices but with restrictions applied to the phone.
- Provide company-issued devices. This provides employees with the convenience of the applications provided by these devices but use is more easily restricted and employee privacy issues are eliminated.
- Forbidding the use of non-company-issued mobile devices for work-related tasks – including for personal productivity gains such as note-taking.

Regardless of the approach you choose, it is vital that the security policy be updated to reflect the organization's stance on BYOD. This policy update must be communicated to all employees along with the ramifications of not adhering to the policy.

What you want to avoid is employees freely using their own device without restriction or a policy for the use of the device. Typically this only occurs when an organization has not yet addressed the issue of BYOD, is in denial that BYOD is an issue or doesn't fully understand the security and privacy implications of BYOD.

Your Security Policy

Regardless of whether you allow BYOD, your organization provides the mobile device, or you forbid the use of mobile devices, you'll want to update your organization's security policy specifically to address the issue. You should carefully go over the policy with the employee, making sure they understand each point. Here are some of the examples of the issues to cover when allowing the use of mobile devices, realizing that the details of these issues will be different depending on whether the device is the employee's or the organization's.

Reminder of the acceptable uses of the device itself and specifically of your organization's data. For example, a reminder that posting corporate data and company confidential information to social media and file sharing website is not acceptable.

- Encryption requirements – both for connections and storing of data (if allowed.)
- Who pays for the device and/or the monthly carrier fees
- Who provides support
- Action taken against the device (and its contents – including personal data) when:
    - the device is lost or stolen
    - the employee leaves the organization
    - the employee is terminated
    - an invalid security code to unlock the device is entered too many times

    Most organizations wipe (delete) all data (including users' personal data) when any of these events occur. If the device is the employee's and they refuse to allow this, most organizations refuse to allow the employees to participate in a BYOD program. However you choose to handle this, the employee must be fully aware of and agree to this policy. To wipe their phone without their consent may be a violation of the employee's privacy. (Note, this section must be a list of *all* events that trigger a lock-out or deletion of data.)
- What happens to the device if its contents is required for discovery in the context of litigation involving the organization. What contents will be examined.
- If you are restricting access to certain applications, this should be articulated or provide an indication of where the current restriction list can be obtained.
- Under what circumstances are the applications used and the employee's location tracked.

This list is not meant to be an exhaustive list of issues to address. Make sure that this section of security policy completely meets your organization's needs and legal requirements. To that end, I highly recommend that your security policy – and this section specifically - be reviewed with your legal counsel.

Conclusion

Security is about trade-offs. Use of mobile devices requires trade-offs between unrestricted use and protecting your organization. Your goal should be to find a method that reduces the risk of compromising your organization's data while allowing the use and convenience of mobile devices.

The solution to the security and privacy issues surrounding BYOD and mobile device security is going to vary from organization to organization. Hopefully I've provided you with an overview of the issues, a place to start researching technology and ideas on how to address the issue within your organization.

Carol Woodbury is President and co-founder of SkyView Partners, Inc, a firm specializing in security administration and compliance software, consulting and managed services for IBM i, AIX and Linux. Carol is the former Chief Engineering Manager of Security Technology in Rochester, MN and has over twenty years' experience in the area of computer security. Carol is an internationally-known and award-winning speaker and writer in the area of computer security. Carol's fourth book, IBM i Security Administration and Compliance is a top-selling reference for many IBM i organizations. Carol is Certified in Risk and Information Security Control (CRISC.)