

Background  
&  
Stakeholders

Security,  
Privacy &  
Legal

Enterprise  
Mobility  
Management

Financial

Interviews &  
Case  
Studies

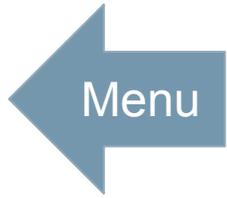
Recommend  
ation

# Bring Your Own Device: An Interactive Report

Carnegie Mellon University, Heinz College, Spring 2015

Designed by Ronald Chang

Content by Jenai Booker, Shifang Peng, Sarat Meduri, Juan German



Bring Your Own Device

Benefits for City of Pittsburgh

Unionized Workforce Concerns

Stakeholders

# Bring Your Own Device

The development of modern devices such as smartphones and tablets has triggered drastic changes in work-style and workplace. Bring-Your-Own-Device (BYOD) programs, which refer to the use of employee-owned devices to access enterprise content or networks, have resulted from the increasing importance of smart devices usage. The Ponemon Institute reported that growth in organizations adopting a BYOD strategy has increased by 73% in the last four years. It was predicted that up to 90% of organizations will encourage employees to use their own electronic mobile devices and support the use of corporate software applications on those devices by 2014. BYOD has become a trend that it is not only applicable to the private sector, but also is being embraced by the public sector, embodied by organizations on the federal, state, and local government level. BYOD is also growing popular in the education and healthcare fields across numerous other countries including the UK, Germany, China, and India.

## Top 3 Resources for General BYOD

1. [The “Bring Your Own Device” To Work Movement](#) -- Littler
2. [Understanding The BYOD Landscape](#) -- Deloitte
3. [Addressing the Challenges of the ‘Bring Your Own Device’ Opportunity](#) -- The CPA Journal

BYOD

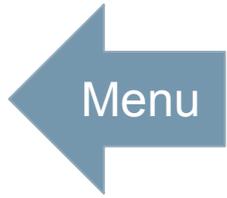
EMM

INFO  
SEC

COST

CASE  
S

REC



# Benefits for City of Pittsburgh

Bring Your Own Device

Benefits for City of Pittsburgh

Unionized Workforce Concerns

Stakeholders

The City of Pittsburgh is estimating the feasibility of BYOD implementation across city departments and needs objective information about the overall vision of BYOD in government, as well as a comparison of BYOD implementation experiences among governments and organizations equivalent in size. Based on our assessment of cities that have implemented a BYOD, the overall benefits that are potentially applicable to the City of Pittsburgh are observed improvements in mobility, employee satisfaction, ease of device management, and organization productivity. These benefits are substantiated by findings from a 2012 CDW-G report indicating that 89 percent of federal employees who use a mobile device for work say it makes them more productive, as well as a 2012 GovLoop survey of federal, state, and local government agencies showing that 58 percent of respondents cited improved productivity as a benefit of BYOD policies.

### Top 3 Resources for General BYOD

1. [The “Bring Your Own Device” To Work Movement](#) -- Littler
2. [Understanding The BYOD Landscape](#) -- Deloitte
3. [Addressing the Challenges of the ‘Bring Your Own Device’ Opportunity](#) -- The CPA Journal

BYOD

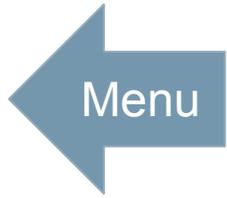
EMM

INFO  
SEC

COST

CASE  
S

REC



# Unionized Workforce Concerns

Bring Your Own Device

Benefits for City of Pittsburgh

Unionized Workforce Concerns

Stakeholders

The City of Pittsburgh is concerned with BYOD compliance issue for unionized employees including police, fire, public works and others, since the union protects employees' working rights in terms of work hours, privacy rights, etc. Unions have the resources to mobilize their members, file lawsuits and draw a significant amount of negative publicity, potentially causing serious reputational damage to the organization.

To address this issue, attention needs to be paid at first to consulting the terms of the collective bargaining agreement covering the employees to determine if there are any applicable restrictions. A policy for a unionized workforce need not be identical to a policy for the employer's non-unionized workforce and may provide for different restrictions or rights.

Therefore, when pressure from union is considered, it is suggested that the employer needs to specify policies that fully segregate personal and work spaces on dual purpose mobile devices prior to a BYOD implementation.

## Top 3 Resources for General BYOD

1. [The "Bring Your Own Device" To Work Movement](#) -- Littler
2. [Understanding The BYOD Landscape](#) -- Deloitte
3. [Addressing the Challenges of the 'Bring Your Own Device' Opportunity](#) -- The CPA Journal

BYOD

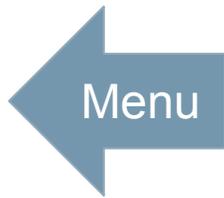
EMM

INFO  
SEC

COST

CASE  
S

REC



Bring Your Own Device

Benefits for City of Pittsburgh

Unionized Workforce Concerns

Stakeholders

Stakeholders	Impacts	Perceived Attitudes	Stakeholder Management Strategy	Role
Executive Decision Makers: Mayor, CIO, CAO, CIPO, CLO	High	Supportive	<ul style="list-style-type: none"> <li>Involvement in project steering committee and meeting with I&amp;P staff</li> </ul>	<ul style="list-style-type: none"> <li>Program decision makers and potential facilitators (if BYOD is "yes")</li> </ul>
Law Department	High	TBD	<ul style="list-style-type: none"> <li>Involvement in BYOD policy formulation and cooperation and coordination with I&amp;P</li> </ul>	<ul style="list-style-type: none"> <li>Legal policies formulator</li> <li>Legal consultant</li> </ul>
Department of Innovation & Performance (I&P) and Office of Management & Budget (OMB)	High	TBD	<ul style="list-style-type: none"> <li>Involvement in analyzing findings, facilitating the implementation (if BYOD is "yes") and coordinating with multiple departments in the process of testing the feasibility of a BYOD program in the City of Pittsburgh</li> </ul>	<ul style="list-style-type: none"> <li>Primary BYOD supervisor, feasibility researcher, and BYOD proposer</li> <li>Key driver for implementing a BYOD program (if BYOD is "yes")</li> <li>Security policies formulator</li> </ul>
Department of Finance and Office of Management & Budget (OMB)	Medium	TBD	<ul style="list-style-type: none"> <li>Involvement in budget plan for the BYOD program and coordination with I&amp;P regarding financial issues</li> </ul>	<ul style="list-style-type: none"> <li>Key participant in the process of BYOD planning</li> </ul>
Non-Unionized:				
Administrators and Managers	Medium	TBD	<ul style="list-style-type: none"> <li>Involvement in the process of decision-making. Need their opinions for identifying the impacts of BYOD</li> </ul>	<ul style="list-style-type: none"> <li>Potential BYOD drivers in departments (if BYOD is "yes")</li> <li>BYOD participants</li> </ul>
Professional	Low	TBD	<ul style="list-style-type: none"> <li>Need their feedbacks in the process of BYOD decision-making</li> </ul>	<ul style="list-style-type: none"> <li>BYOD participants</li> </ul>
Unionized:				
Police	Low	Concerned	<ul style="list-style-type: none"> <li>Need feedback in the process of BYOD decision-making</li> </ul>	<ul style="list-style-type: none"> <li>BYOD participants</li> <li>Potential BYOD opponents (need further evidence)</li> </ul>
Fire	Low	Concerned	<ul style="list-style-type: none"> <li>Need feedback in the process of BYOD decision-making</li> </ul>	<ul style="list-style-type: none"> <li>BYOD participants</li> <li>Potential BYOD opponents (need further evidence)</li> </ul>
Public Works	Low	Concerned	<ul style="list-style-type: none"> <li>Need feedback in the process of the BYOD decision-making</li> </ul>	<ul style="list-style-type: none"> <li>BYOD participants</li> <li>Potential BYOD opponents (need further evidence)</li> </ul>
Others	Low	Concerned	<ul style="list-style-type: none"> <li>Collect feedback from them</li> </ul>	<ul style="list-style-type: none"> <li>BYOD participants</li> </ul>

BYOD

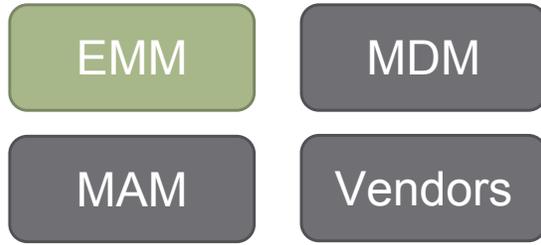
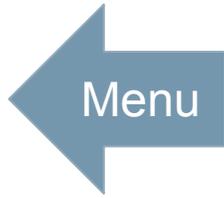
EMM

INFO SEC

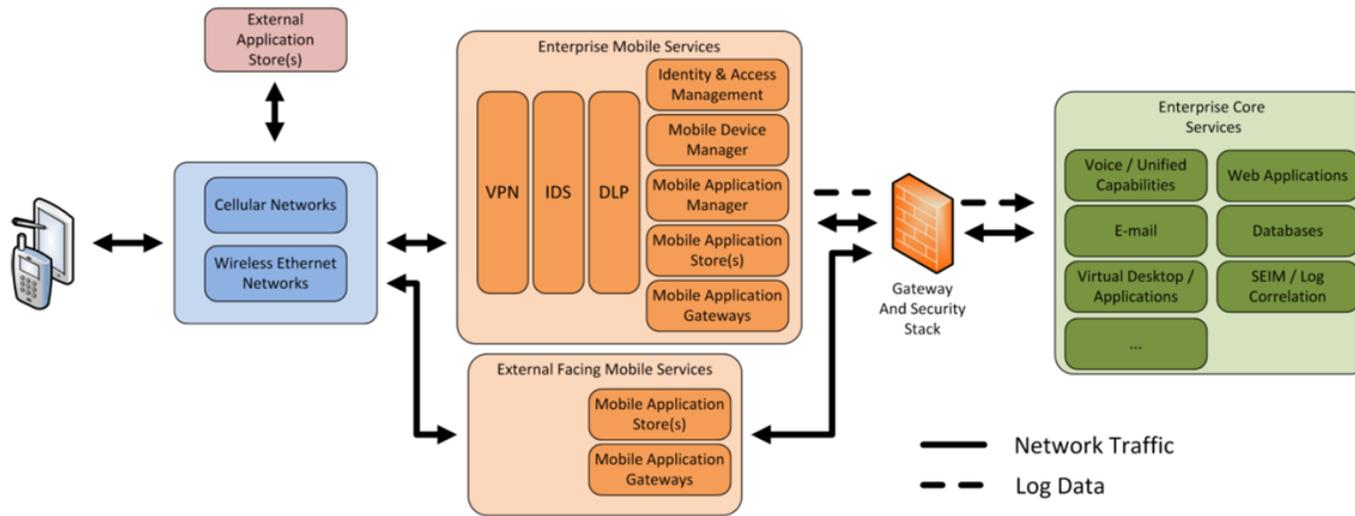
COST

CASE S

REC



# Enterprise Mobility Management



Various technology solutions are available to address the many different concerns that an organization and its employees may have when implementing BYOD. Each technical approach vary in how they address these concerns. Each carry their own benefits, costs, risks, and requirements.

### Concerns:

- *costs*
- *security*
- *privacy*
- *user experience*
- *functionality*
- *management*

### Top 3 Resources on BYOD Technology

1. [Mobile Security Reference Architecture](#) – DHS & CIO
2. [Best BYOD management: Containment is your friend](#) -- Computerworld
3. [BYOD: Why Mobile Device Management Isn't Enough](#) -- InformationWeek

The figure on the left, taken from the Department of Homeland Security's Mobile Security Reference Architecture, depicts where enterprise mobility management fits.

BYOD

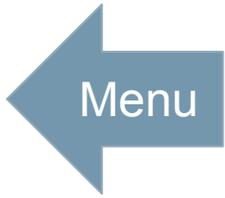
EMM

INFO SEC

COST

CASE S

REC



EMM

MDM

MAM

Vendors

# Mobile Device Management

Costs

Security vs. Privacy, UX, Functionality

Management

Limitations

## Costs

Limited separation approach can be the least costly solution, due to the lack of requirements and the ease in which it can adapt to existing infrastructure. A personal device can simply be configured to retrieve emails, contacts, and calendars from the organization's hosted servers. Most smartphones, especially those that come with the most popular two operating systems, Apple's iOS and Google's Android, have native support for this function.

In a limited separation approach, it is difficult to distinguish calls and bandwidth usage that is work-related and usage that is personal. This means that the organization must determine a program that is cost-efficient for the organization while fair for the employee.

## Limited Separation

The most common form of BYOD due to its informality and lack of required support infrastructure to implement it. Organizations can use Microsoft's Exchange ActiveSync to allow their employees access to Exchange email, contacts, and calendar. These features work on the user device's native applications, alongside their personal email, contacts, and calendar. Typically, organizations that do manage personal devices with a limited separation approach do so with an MDM solution because controls are implemented at the device level.

BYOD

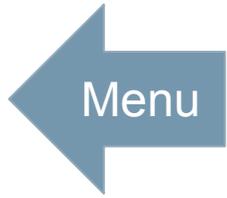
EMM

INFO SEC

COST

CASE S

REC



EMM

MDM

MAM

Vendors

# Mobile Device Management

Costs

Security vs. Privacy, UX, Functionality

Management

Limitations

## Security vs. Privacy, UX & Functionality

With MDM, features that can boost the organization's security can infringe on the user's privacy, user experience, and the functionality of their device. Since an organization's data resides on an employee's device, the employee surrenders and even loses personal data in investigations or when the device is remote-wiped if it falls out of compliance since personal data and work are not separated. Password requirements can also significantly impacting the user experience. These security features that conflicts with privacy, user experience, and functionality of the user's device makes BYOD unacceptable for many.

## Limited Separation

The most common form of BYOD due to its informality and lack of required support infrastructure to implement it. Organizations can use Microsoft's Exchange ActiveSync to allow their employees access to Exchange email, contacts, and calendar. These features work on the user device's native applications, alongside their personal email, contacts, and calendar. Typically, organizations that do manage personal devices with a limited separation approach do so with an MDM solution because controls are implemented at the device level.

BYOD

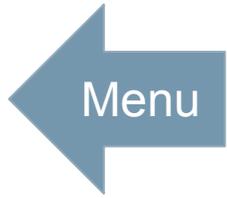
EMM

INFO SEC

COST

CASE S

REC



EMM

MDM

MAM

Vendors

# Mobile Device Management

Costs

Security vs. Privacy, UX, Functionality

Management

Limitations

## Management

The traditional and most common approach to managing mobile devices in an enterprise environment is to have them managed through MDM solutions from a third party. The technology allows an organization to centrally manage and control the many mobile assets used in a work environment throughout the device lifecycle, from provisioning devices to recycling them. MDM has been used in the past to manage standardized corporate mobile devices and have been adapted to allow for non-proprietary devices. Through MDM technology, an organization can centrally distribute applications, data, configuration settings, and software updates over wireless networks. More importantly, an organization can manage the different security challenges presented before across all devices using device policies, data encryption, and authentication.

## Limited Separation

The most common form of BYOD due to its informality and lack of required support infrastructure to implement it. Organizations can use Microsoft's Exchange ActiveSync to allow their employees access to Exchange email, contacts, and calendar. These features work on the user device's native applications, alongside their personal email, contacts, and calendar. Typically, organizations that do manage personal devices with a limited separation approach do so with an MDM solution because controls are implemented at the device level.

BYOD

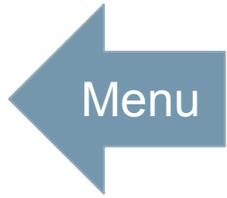
EMM

INFO SEC

COST

CASE S

REC



EMM

MDM

MAM

Vendors

# Mobile Device Management

Costs

Security vs. Privacy, UX, Functionality

Management

Limitations

## Limitations

Mobile devices are architected in a way that prevents lateral movement. This means that a device-level approach is quite limited in its features and unable to do more granular controls on devices.

MDM also needs to be connected to the device to issue the action. Remote wipes are usually triggered over a network, rather than the device itself.

Finally, encryption and security measures vary across devices. It's hard to standardize encryption and security configurations across all devices.

## Limited Separation

The most common form of BYOD due to its informality and lack of required support infrastructure to implement it.

Organizations can use Microsoft's Exchange ActiveSync to allow their employees access to Exchange email, contacts, and calendar. These features work on the user device's native applications, alongside their personal email, contacts, and calendar. Typically, organizations that do manage personal devices with a limited separation approach do so with an MDM solution because controls are implemented at the device level.

BYOD

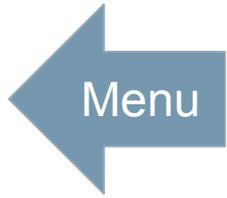
EMM

INFO SEC

COST

CASE S

REC



EMM

MDM

MAM

Vendors

# Mobile Application Management

Containerization

Security,  
Privacy,  
Functionality

Costs

Limitations

Virtualization

## Features

- app wrapping
- granular device controls.
- app delivery, version management, and updates via app store
- app configuration management and push services
- event management, usage analytics, crash reporting and tracking
- offline software policies.
- user authentication and single sign-on integration.
- geo-fencing
- user and group access control
- over-the-air and local encryption.

## Management

Due to the heavy-handed nature of a MDM approach, MDM vendors have started taking an application-focused approach to BYOD. Rather than manage and control devices, mobile application management (MAM) has a higher level of control over applications installed on devices. This allows for software level containerization and virtualization approaches to BYOD that allow for greater privacy, more flexibility, and better user experience without jeopardizing security. Most organizations that use MAM extend beyond the use of email and have started developing internal applications to support their business, taking advantage of the flexibility and security that MAM allows.

MAM software services have many of the same features as MDM software services. However, unlike MDM, MAM targets the software level of the device, rather than the entire device itself. This allows for more granular control since software can be run on most devices and standardized to work the same regardless of which device manufacturer and version.

BYOD

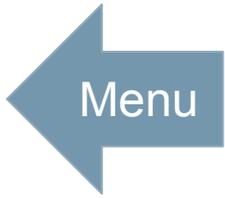
EMM

INFO  
SEC

COST

CASE  
S

REC



EMM

MDM

MAM

Vendors

# Mobile Application Management

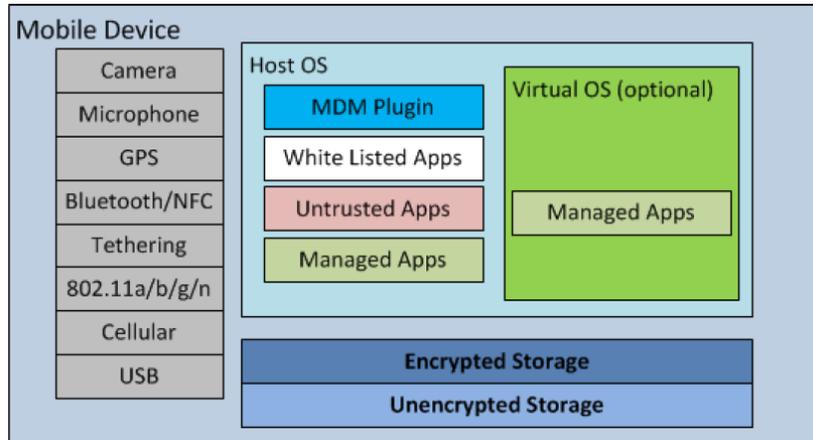
Containerization

Security, Privacy, Functionality

Costs

Limitations

Virtualization



## Containerization

Also known as a “walled-garden”, the containerization approach to BYOD is allotting space on a personal device for work-related applications and data. This secure and encrypted container is completely separate from the rest of the device and has more restrictive security measures to prevent data leakage. Containerization is implemented in three different ways:

1. Encrypted space for work applications and data
2. Using an app wrapper to secure corporate applications and data
3. Create a virtual work phone using mobile hypervisors.

BYOD

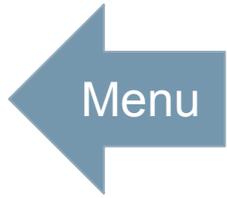
EMM

INFO SEC

COST

CASE S

REC



EMM

MDM

MAM

Vendors

# Mobile Application Management

## Security, Privacy, Functionality

This approach makes BYOD much more acceptable for employees because the sacrifices are much more minimal. All the security policies and restrictions are in place at the software level and only apply to applications and data that is within the container. That means that the employees still get to use their devices and all its functionality as they normally would while only sacrificing some storage capacity. Compliance policies that would trigger remote wipes or password requirements only apply to the container on the device. If the organization required that the camera be disabled or that copy and paste functionality is disabled, it would only be applicable in applications that are work-related. While it varies depending on the implementation, containerization can be thought of as a separate and more secure device within the user's personal device. However, many containerization solutions are unable to detect whether or not the device is rooted or jailbroken. This means that security measures placed on the phone would be meaningless if the user finds a way to circumvent the device manufacturer's operating system and security model. A jailbroken or rooted device leaves the device and data stored in containers vulnerable to exploitation by malicious applications.

Containerization

Security,  
Privacy,  
Functionality

Costs

Limitations

Virtualization

BYOD

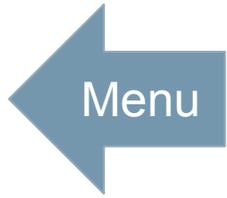
EMM

INFO  
SEC

COST

CASE  
S

REC



EMM

MDM

MAM

Vendors

# Mobile Application Management

Containerization

Security,  
Privacy,  
Functionality

Costs

Limitations

Virtualization

## Costs

The use of MAM to implement containerization saves the organization time since the IT department does not need to certify and support a list of devices, but rather, design applications that would work across all devices. This means support for wider range of devices since the software is designed to run on multiple platforms. Unlike the heavy-handed approach of MDM, containerization is often more acceptable to users and should see greater adoption rates, encouraging employees to use their own devices rather than corporate-issued devices. Assuming that the reimbursement plans and licensing costs have been calculated to be cost-effective for the organization, this translates to a reduction in expenses.

For a rough estimate on licensing costs for a containerization solution, AirWatch by VMware, a leader in the enterprise mobility management services space, prices their licenses \$50 to \$130 per device, depending on the set of features their customers are interested in and where the services are hosted. Alternatively, organizations can pay per user, which costs \$102 to \$220 per user. With nearly 3,000 employees, the City of Pittsburgh could spend approximately \$225,000 on licensing alone per year for AirWatch's Blue Management Suite if the MAM solution is deployed on the cloud. Key features of AirWatch's Blue Management Suite would include app wrapping, a secure browser, email, and app catalog. This figure also assumes that the City of Pittsburgh would, in turn, have no costs associated with procuring devices for employees.

BYOD

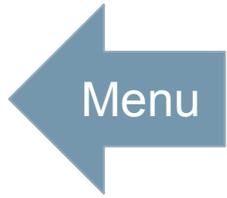
EMM

INFO  
SEC

COST

CASE  
S

REC



EMM

MDM

MAM

Vendors

# Mobile Application Management

Containerization

Security,  
Privacy,  
Functionality

Costs

Limitations

Virtualization

## Limitations

While app wrapping provides a layer of security and control to each individual application, it requires access to modify the application's binary code in order to wrap it. Unless the application was developed internally or is freely available, the organization will need to partner with the application developers in order to wrap the desired application. This is especially difficult with native applications on iOS and Android devices since the device manufacturers are unlikely to allow their applications to be modified. However, device manufacturers such as Apple and Google are working on allowing app wrapping on applications on their devices.

Another downside to containerization is that many of the commercial products are incompatible with Apple devices, particularly dated devices from older generations. This is especially an issue because in enterprises, Apple has 60% market share compared to Android's 10%. The products that do support Apple products have issues keeping up to date with Apple's patch releases due to Apple's secretive nature about their updates. This means that users cannot upgrade their operating system to the latest release until the BYOD provider has updated, tested, and ready to release a new version that is compatible.

BYOD

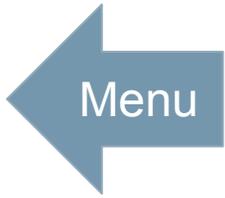
EMM

INFO  
SEC

COST

CASE  
S

REC



EMM

MDM

MAM

Vendors

# Mobile Application Management

Containerization

Security,  
Privacy,  
Functionality

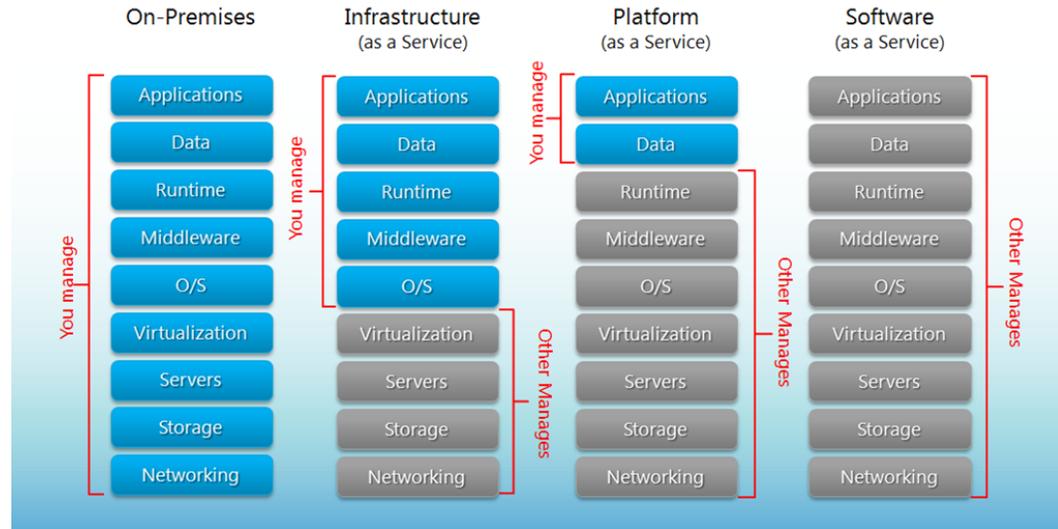
Costs

Limitations

Virtualization

## Virtualization

Virtualization is a term to describe technology that creates virtual instances rather than being connected directly to the underlying hardware. This concept of virtualization can be further abstracted where hardware and even software resources are hosted in another location altogether. This is commonly referred to as cloud computing, where the processing power and software are hosted on a server (or servers) and delivered to a device through an internet connection. In a way, the application running on the device is a window into software running on a separate computer.



In the context of BYOD, through virtualization, an application on a mobile device can connect securely to resources hosted over the internet and access information without any data stored on the device itself. For an organization, virtualization means they do not have to manage the device nor the applications. Rather, they focus on managing access to services hosted by the organization internally or a third-party vendor.

BYOD

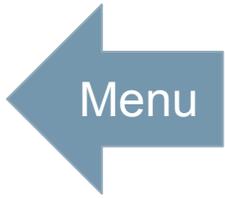
EMM

INFO SEC

COST

CASE S

REC



EMM

MDM

MAM

Vendors

VMWare AirWatch

Citrix XenMobile

Soti MobiControl

Blackberry BES10

SAP Afaria

AT&T Toggle

There are many players in the enterprise mobility management space, many of which deliver similar services but some offer unique features that distinguishes them from their competitors. Gartner’s Magic Quadrant for Enterprise Mobility Management Suites report in June 2014 shows EMM providers ranked based on their ability to execute and their vision. Vendors that can execute are those that ensures complete implementation and reliable service. Vendors that rank highly in “completeness of vision” are those that understand the market and respond effectively with innovative products and services.

# Vendors



### Top 3 Resources on MDM Vendors

1. [Comparison of MDM Providers](#) – Enterprise iOS
2. [Magic Quadrant for Enterprise Mobility Management Suites](#) – Gartner
3. [Mobile Device Management: Vendors and Comparison Guide](#) – Tom’s IT Pro

BYOD

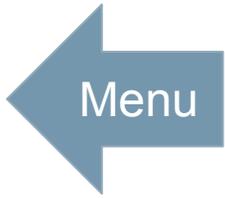
EMM

INFO SEC

COST

CASE S

REC



EMM

MDM

MAM

Vendors



VMWare AirWatch

Citrix XenMobile

Soti MobiControl

Blackberry BES10

SAP Afaia

AT&T Toggle

AirWatch, acquired by VMWare in 2014, is currently the market leader in the enterprise mobility management space, according to Gartner Magic Quadrant report in 2014 (Figure 4). Offering both cloud-based and on-premise deployments, AirWatch has a broad range of services and accommodates different solutions that organizations are looking for. Their containerization approach through Workspace Management, which is separated and secured on the device, deploys email, internet browsing, data storage, and other apps as stand-alone applications. AirWatch is also compatible with any possible mobile device, supporting Android, Apple iOS, BlackBerry, and Windows. A cloud-based subscription license starts at \$51 per device annually for the most basic features on top of the \$1,500 for deployment services. For the highest level suite, it can cost \$110 per device annually, with \$6,500 in deployment costs.

BYOD

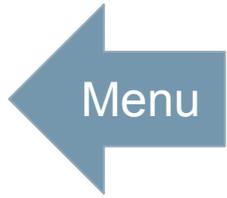
EMM

INFO SEC

COST

CASE S

REC



EMM

MDM

MAM

Vendors

CITRIX  
XenMobile

VMWare AirWatch

Citrix XenMobile

Soti MobiControl

Blackberry BES10

SAP Afaria

AT&T Toggle

Citrix XenMobile offers many of the same features as VMWare's AirWatch. However, Citrix, being a leader in virtualization, allows organizations to deploy native applications, which would otherwise be incompatible with mobile devices, through the Citrix Unified App Store. An organization's IT department can easily wrap any application to make it accessible to mobile devices. Some other unique features of XenMobile is "geo-fencing" and root or jailbreak detection. Geo-fencing is the use of geolocation on the device to limit the geographical location in which the device can access work-related files. XenMobile also uses hardware and software level mechanisms to detect whether a device is jailbroken or rooted. An organization can then trigger a lock or remote wipe if the device falls out of compliance.

BYOD

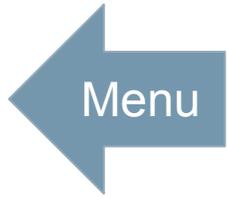
EMM

INFO  
SEC

COST

CASE  
S

REC



EMM

MDM

MAM

Vendors

VMWare AirWatch

Citrix XenMobile

Soti MobiControl

Blackberry BES10

SAP Afaria

AT&T Toggle



SOTI®  
**MobiControl**®

SOTI MobiControl is similar to many MDMs in features but differentiates itself by working to address Android fragmentation, an issue where Android devices are so different from one another that it is difficult to develop software for devices with such variation. SOTI works closely with Android partners to develop MobiControl's Android+ Technology that effectively manages the different variations among Android devices. MobiControl also features jailbreak and root detection.

BYOD

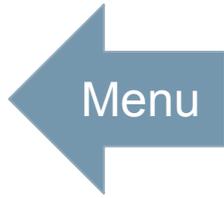
EMM

INFO  
SEC

COST

CASE  
S

REC



EMM

MDM

MAM

Vendors

VMWare AirWatch

Citrix XenMobile

Soti MobiControl

Blackberry BES10

SAP Afaia

AT&T Toggle

## BlackBerry Enterprise Service 10

Many organizations already have a BlackBerry infrastructure in place where a majority of corporate issued devices are BlackBerry phones. If this is the case, BlackBerry's BES10 EMM suite might be a cost effective and convenient option for BYOD now that they have expanded support to include Android and iOS devices. BlackBerry is rolling out support for Windows devices soon and is also launch a cloud-based version to reduce infrastructure costs. Like the aforementioned EMMs, BES10 supports containerization for Android and iOS devices, separating the user's personal data and applications from the "Secure Work Space", the device's work related environment where users can securely access email, documents, content, and apps. However, the features for non-BlackBerry devices are still limited relative to the other EMMs. Depending on the features required, licensing ranges from \$19/year per device to \$60/year per user.

BYOD

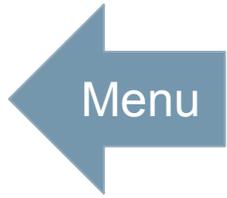
EMM

INFO  
SEC

COST

CASE  
S

REC



EMM

MDM

MAM

Vendors

VMWare AirWatch

Citrix XenMobile

Soti MobiControl

Blackberry BES10

SAP Afaria

AT&T Toggle



SAP, the enterprise software giant, focuses more on ensuring data security with their EMM, Afaria. SAP Afaria encrypts and validates all data that traverses the network, assuring that communications are secure and authorized. Afaria combines hardware, software, and content mechanisms to address the security needs of an organization, such as the detection and protection against jailbreak or rooted devices in the enterprise environment. Similar to other EMMs, Afaria also features an enterprise application store that allows users to download and install authorized applications onto their mobile device.

BYOD

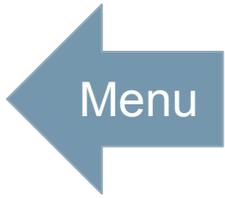
EMM

INFO  
SEC

COST

CASE  
S

REC



EMM

MDM

MAM

Vendors



**AT&T Toggle**<sup>®</sup>

*A highly secure BYOD solution*

VMWare AirWatch

Citrix XenMobile

Soti MobiControl

Blackberry BES10

SAP Afaia

AT&T Toggle

AT&T's business division offers a cloud-based BYOD solution called "Toggle" that uses Type 2 virtualization to create two identities on one device, one for personal use, and the other for work. While the former is used to personal communications and entertainment, the latter is a password protected workspace used to access corporate email, contacts, calendar, and applications. A unique feature of Toggle is support of two phone numbers, which allow employees to separate minutes that are work related from personal calls. The separate phone identities also allows separation of data usage so employees aren't responsible for work related data usage. Toggle is carrier agnostic so it does not require AT&T to be the service provider. It currently supports Android and iOS, with Windows and BlackBerry support on its way. Toggle is a very expensive option however, at \$750 setup fee per device, and a \$6.50 monthly fee per device. Additional support adds another \$1.50 to \$2.50 per month for each device.

BYOD

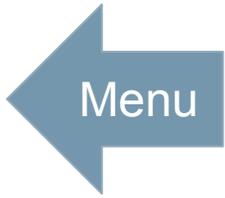
EMM

INFO  
SEC

COST

CASE  
S

REC



Security

Legal

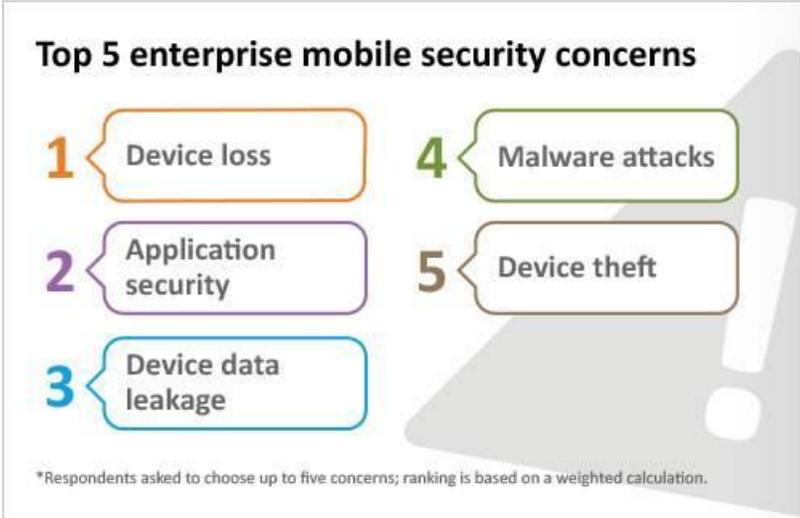
Privacy

# Security

Loss of Device

Application Security Management

Mobile Malware



In BYOD, the employee owns the device. However, when it comes to managing and securing the device, contentious issues start to crop up because the device, though owned by the user, carries both personal as well as the organization's data. Hence, both the user and the company are now stakeholders in securing the device as both stand to lose due to any security threats to the device directly or to the data on the device.

So the question is, in a nutshell, given all of the above constraints, how does one securely enable access to enterprise apps and resources and give those end users that speed of access that they want and the ease of access that they want, but still maintain security.

BYOD

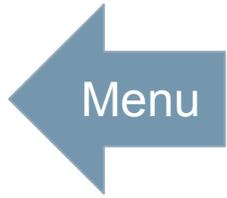
EMM

INFO SEC

COST

CASE S

REC



Security

Legal

Privacy

# Loss of Device

Loss of Device

Application Security Management

Mobile Malware

Mobile devices get lost more often than PCs due to their smaller form factor, which means users tend to bring them everywhere. Under such circumstances, the loss of a device with potentially sensitive work-related data on it is a huge security risk for any organization.

Thus, having the option of either locking down/ deactivating a device (carrying sensitive work data) upon knowing that it has been stolen or better yet, the ability to remote wipe a device is crucial in managing such tricky situations. If a company can remote wipe the data, then the threat due to loss of data can be managed. Now, in order to wipe the organization's data off a stolen phone, IT should not have to remotely wipe all the data from it. This is especially pertinent when an employee is leaving the firm and the organization's data has to be removed from the device. This situation calls for the expertise of granular remote wiping, which means only the work related data is wiped and not the personal data. IT should not have to remote wipe the user's personal data like their personal email or family vacation photographs on their phones just to get the company's data off the phone.

Thus, to effectively manage such situations, organizations need a mechanism that would allow them to lock down devices when they realize they have been stolen and more importantly, a mechanism that allows companies to remote wipe devices as and when required.

BYOD

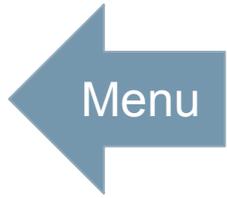
EMM

INFO SEC

COST

CASE S

REC



Security

Legal

Privacy

# Application Security Management

Loss of Device

Application Security Management

Mobile Malware

In a BYOD setting, a user needs to be very careful before downloading an app because malware introduced through downloading a faulty app could affect all the data on the entire device.

Whitelists and Blacklists of Apps

The employees need to have a clear picture of which apps can be downloaded and those that cannot be in order to ensure application security and security in general. The modern trend is to look for enforced blacklists, based on known information about those apps, which prohibit users from downloading those apps. Also, whitelists can be maintained that specify to the user that those apps are clean and can be downloaded. One aspect that is gaining currency of late is the concept of in house “app stores”, where the organization’s IT team maintains and manages its own app store from where the user gets their applications.

BYOD

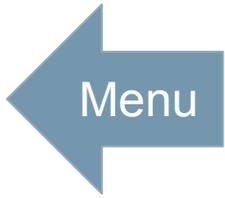
EMM

INFO SEC

COST

CASE S

REC



Security

Legal

Privacy

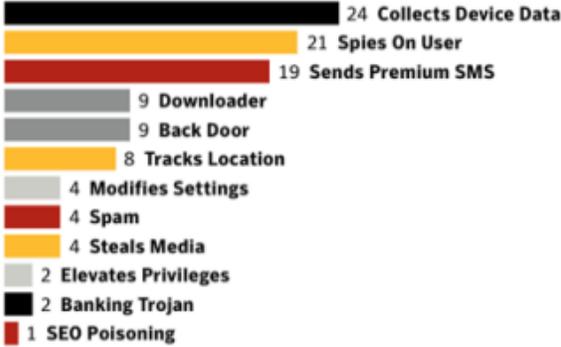
# Mobile Malware

Loss of Device

Application Security Management

Mobile Malware

Mobile Threats: Malicious Code By Type – Additional Detail, 2011



Source: Symantec

### Potential Mobile Threat Vectors

- **Trojanized apps** from cybercriminals can infect devices
- **Embedded links in SMS, social media, and email links** can potentially redirect users to websites that host malicious files.
- **Third-party app stores** may host malware that can potentially harm devices, systems, and networks.

The smartphone (or tablet) presents an excellent platform for advanced and persistent attacks either to gain access to sensitive data or to trick the user into giving up their credentials by accessing fraudulent sites. The threat is not only growing in volume, but also in complexity.

In fact, malware infections in mobile device increased by 25 percent last year and mobile malware is becoming more sophisticated with robust command and control protocols. That malware can be used for espionage, data theft, denial of service attackers, and banking and advertising scams. Added to this is the threat of spyware, which is dangerous because it can track a person's browsing history, data on their hard drive and their physical location.

BYOD

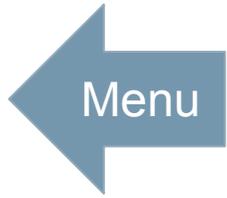
EMM

INFO SEC

COST

CASE S

REC



Security

Legal

Privacy

# Legal

Terms and Conditions Agreement

Acceptable Use

Devices and Support

Expectation of Privacy

Employee Reimbursement

Security and Data Ownership

Risks, Liabilities, Disclaimers

After outlining what an organization is capable of enforcing and developing as many preventative controls as possible that can aid in that enforcement, it is important to draft a terms and conditions contract. This is a central piece of BYOD program development. This contract is the physical manifestation of intricate policy planning. It is important that the content of each of the following sections is considered carefully before the drafting process is initiated.

BYOD

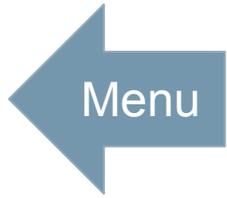
EMM

INFO SEC

COST

CASE S

REC



Security

Legal

Privacy

# Legal

Terms and Conditions Agreement

Acceptable Use

Devices and Support

Expectation of Privacy

Employee Reimbursement

Security and Data Ownership

Risks, Liabilities, Disclaimers

This section of the contract will guide employee behavior after BYOD implementation. It will outline exactly how employees are permitted to use their devices at work.

BYOD

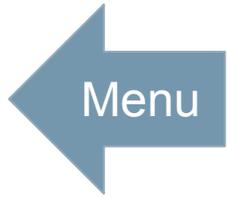
EMM

INFO SEC

COST

CASE S

REC



Security

Legal

Privacy

# Legal

Terms and Conditions Agreement

Acceptable Use

Devices and Support

Expectation of Privacy

Employee Reimbursement

Security and Data Ownership

Risks, Liabilities, Disclaimers

It is also important to communicate which devices will be supported by the IT department. This list of the devices will be updated regularly based on periodic technological updates. It is important to not only to state this information in the terms and conditions agreement, but also to critically think about other issue that may arise as a result of rapid changes in technology.

BYOD

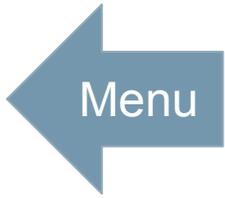
EMM

INFO SEC

COST

CASE S

REC



Security

Legal

Privacy

# Legal

Terms and Conditions Agreement

Acceptable Use

Devices and Support

Expectation of Privacy

Employee Reimbursement

Security and Data Ownership

Risks, Liabilities, Disclaimers

Employers must protect data shared to employee devices. As stated earlier, there are many security concerns in relation to the protection of confidential data. The expectation of privacy section allows the City of Pittsburgh to communicate to employees what actions compromise the security of confidential data.

BYOD

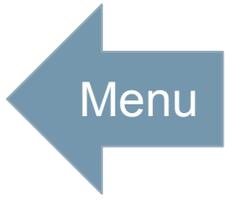
EMM

INFO SEC

COST

CASE S

REC



Security

Legal

Privacy

# Legal

Terms and Conditions Agreement

Acceptable Use

Devices and Support

Expectation of Privacy

Employee Reimbursement

Security and Data Ownership

Risks, Liabilities, Disclaimers

Reimbursement will be a large incentive for employee participation at the initial stage of the program. The sum of the reimbursement will determine how much money the City of Pittsburgh will save by transferring the cost of devices to the employee.

BYOD

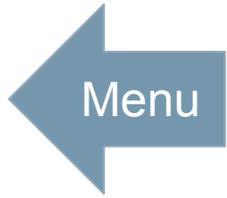
EMM

INFO SEC

COST

CASE S

REC



Security

Legal

Privacy

# Legal

Terms and Conditions Agreement

Acceptable Use

Devices and Support

Expectation of Privacy

Employee Reimbursement

Security and Data Ownership

Risks, Liabilities, Disclaimers

Determining the types of data that is owned by the employer versus owned by the employee is a major hurdle, since it is a very intricate point of this contract drafting process.

BYOD

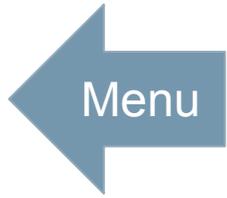
EMM

INFO SEC

COST

CASE S

REC



Security

Legal

Privacy

# Legal

Terms and Conditions Agreement

Acceptable Use

Devices and Support

Expectation of Privacy

Employee Reimbursement

Security and Data Ownership

Risks, Liabilities, Disclaimers

It is vital that employees understand the risks involved with BYOD program prior to participation. This section of the terms and conditions contract is the opportunity to effectively communicate all of the anticipated risk for the employees.

BYOD

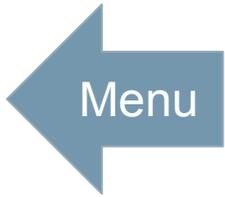
EMM

INFO SEC

COST

CASE S

REC



Security

Legal

Privacy

# Privacy

The BYOD policy in organizations is creating tensions between how much access an employer can have to the worker-owned device and how much privacy an employee can expect. Companies are concerned about security, keeping confidential data from falling into a competitor's hands, and preventing financial account numbers from becoming known to hackers. Employees want to keep prying eyes, including those of their employers, from looking at the photos of their children, text messages from friends and emails from family stored on their mobile devices.

Say an employee, whose iPad device is part of the BYOD program, is at home on a Sunday and is trying to access his/her Facebook profile from the iPad but is shocked to discover that the device refuses to turn on. The employee then learns that his/her little son tried to access a favorite game app on the iPad but entered the wrong passcode thrice and the organization's compliance enforced the lockdown on the device to prevent loss of sensitive data. There was no attempt on the part of the employee to access any work related data and yet, a personal device has been shut down to supposedly protect the organization's data. These are some of the typical privacy concerns that arise when an employee signs up for a BYOD policy in their organization.

BYOD

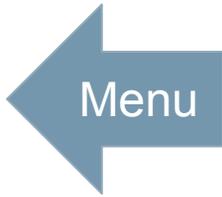
EMM

INFO  
SEC

COST

CASE  
S

REC



# Financial

Financial

Cost Saving Practices

Outlining Specific Policies and Procedures

Tracking Return on Investment

Managing Data Usage

Implementing a BYOD program not only requires consideration of stakeholders, necessary security measures, and a definite device management plan. At the core of all of these components lies the basic requirement of financial support. It is important that among other components, the City of Pittsburgh take extra precaution when approaching the financial aspects of program implementation. It is estimated by analysts at the Aberdeen Group that a BYOD program can cost companies or organizations an average of \$170,000 for every 1000 devices. A lot of this cost was derived from carelessness in every actions during the initial program implementation phase and after the program was launched. This portion of the analysis will outline in detail what these costly actions were and how to incorporate cost saving measures into program implementation, so that a BYOD program does exactly what it is expected to do, save the City of Pittsburgh money.

### Program Savings and Expenses

- device costs
- data and connectivity costs
- security vendor fees
- security and user support costs

### Potential Returns on Investment

- productivity benefits
- availability
- reduced downtime
- reduced distractions
- reduced administration

### Hidden Program Expenses

- transition costs
- subscription costs
- expense reporting costs
- training costs
- support costs
- brand costs
- project rollout costs

BYOD

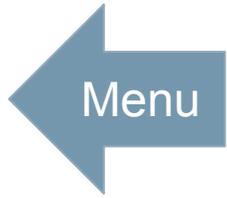
EMM

INFO SEC

COST

CASE S

REC



# Cost Saving Practices

Financial

Cost Saving Practices

Outlining Specific Policies and Procedures

Tracking Return on Investment

Managing Data Usage

If the City of the Pittsburgh anticipates potential hidden costs during the planning process, many of these expensive mistakes can be avoided by outlining specific policies and procedures that address them. In order to successfully reduce cost, it is important that the terms and conditions contract addresses all areas that present a financial concern to the employer. Many of these issues have been outlined in the previous sections, however during the planning process, the committee responsible must brainstorm and critically think about other issues that may become costly.

BYOD

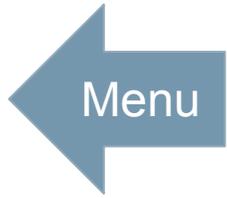
EMM

INFO SEC

COST

CASE S

REC



# Cost Saving Practices

Financial

Cost Saving Practices

Outlining  
Specific  
Policies and  
Procedures

Tracking  
Return on  
Investment

Managing  
Data Usage

Equally as important to saving money, is tracking the return on investment by keeping a detailed records of expenses associated with the program. Tracking every expense will be a colossal and collaborative effort on the part of every department participating in the program. It is important that records are detailed in order to identify areas that need to be reformed in order to gain the largest possible return on investment.

BYOD

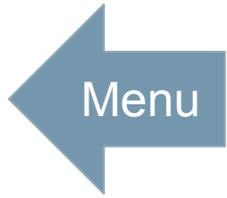
EMM

INFO  
SEC

COST

CASE  
S

REC



# Cost Saving Practices

Financial

Cost Saving Practices

Outlining Specific Policies and Procedures

Tracking Return on Investment

Managing Data Usage

Another crucial cost saving measure is managing the data usage of employees. The acceptable use section of the Terms and Conditions Agreement will be the main source of reference for both employees and employers. In order to enforce the acceptable uses, it is necessary to manage data usage. There will be many parties responsible for making sure that employee uphold their end of the contract. More specifically, that employees use data productively during work hours and without violating the privacy stipulations associated with employee data.

Along with the way that data is used, it is also important to monitor how much data is used. This aspect goes hand in hand with providing employees with limitations on the amount of money that can be designated towards their monthly service fees. By incorporating that limitation into the Terms and Conditions contract, the City of Pittsburgh can avoid much of the cost associated with monitoring and addressing employees who regularly incur overage charges.

BYOD

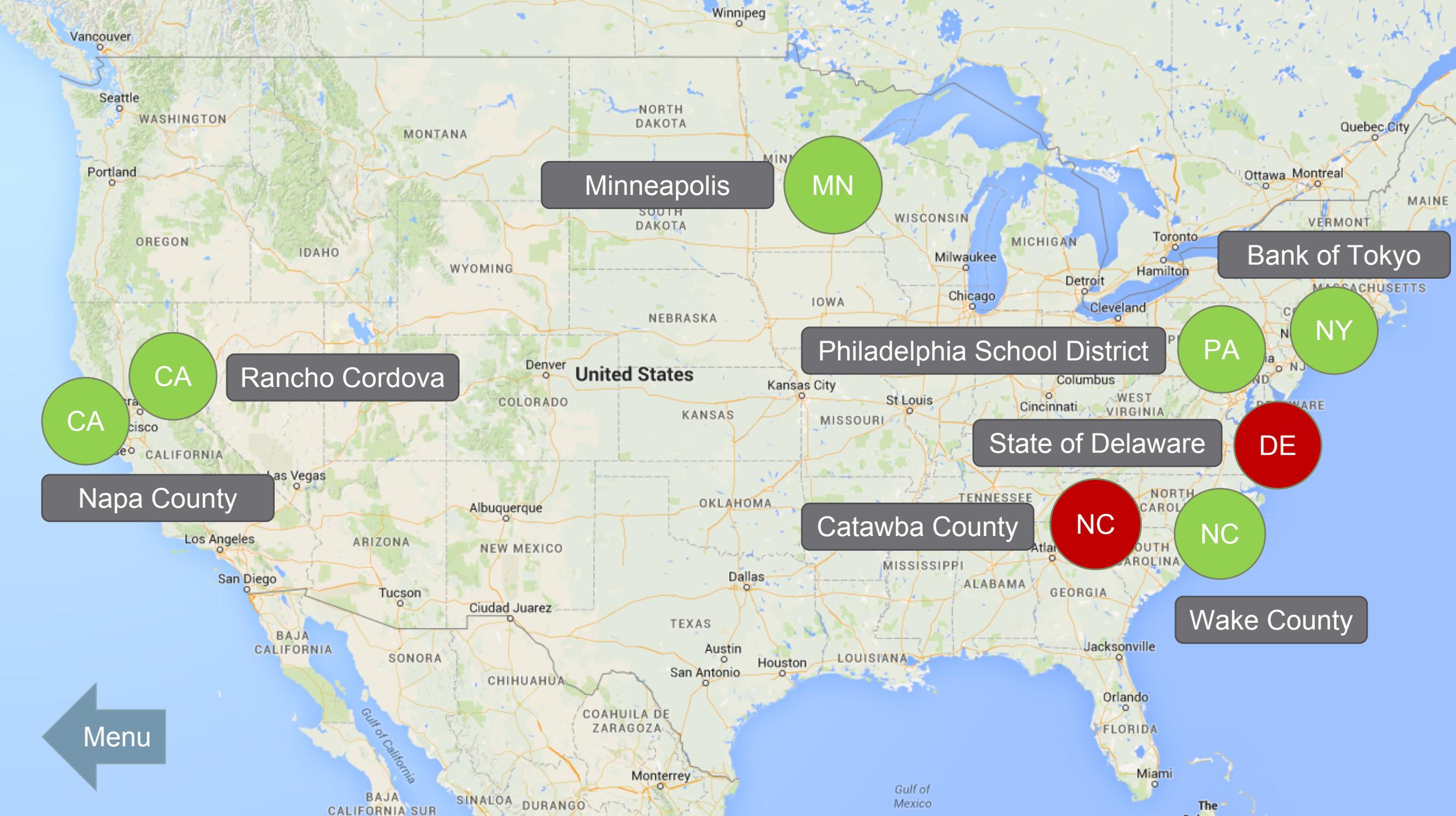
EMM

INFO SEC

COST

CASE S

REC



Minneapolis

MN

Bank of Tokyo

Philadelphia School District

PA

NY

Rancho Cordova

CA

CA

State of Delaware

DE

Napa County

Catawba County

NC

NC

Wake County

Menu

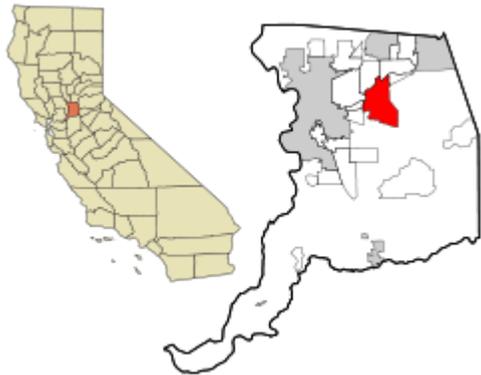


# Rancho Cordova, CA

The City of Rancho Cordova implemented a BYOD program in 2013, because they wanted to eliminate notepads and paper agendas in order to reduce wastage and save money. To achieve these outcomes, the City of Rancho Cordova, CA selected Amtel Integrated Solutions, a leading provider in the management “of cloud-based solutions” for mobile devices and applications in order to help the City implement a successful device management platform.

The city introduced city-owned tablets to their employees and with the expertise of Amtel and their device management products, the tablets enabled staff and city council members to securely share and store agendas, memos and other city-related files in a mobile container. In addition, the city developed a “whitelist” policy of approved applications. Other features include: required employee secure profiles, and passwords (that would be changed every so often in order to minimize data theft). As a result of this initiative, the city eliminated paper wastage and saved nearly \$200,000 annually in printing, paper, and related-costs.

Consequently, the City of Rancho Cordova implemented a Bring Your Own Device program. In this program, employees are encouraged to bring their own device to work as long as it meets the requirements highlighted in the City of Rancho Cordova IT Policy and Procedures: Bring Your Own Device (BYOD) Policy. After implementing the program, the City of Rancho Cordova saw employee productivity and efficiency increased. The reasons were employees knew their devices better, and mobile devices served for more than one function, such as reading emails, taking photos, making calls, accessing data and writing down notes.



For more information visit: <http://www.cityofranhocordova.org/Index.aspx?page=807>

BYOD

EMM

INFO  
SEC

COST

CASE  
S

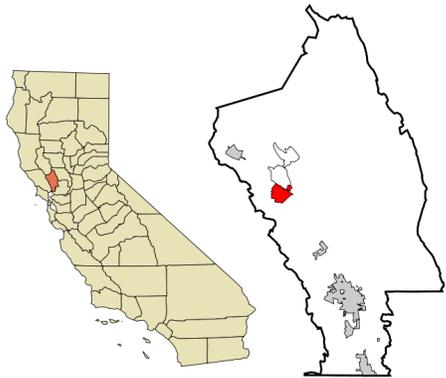
REC



# Napa County, CA

In 2010, the County of Napa implemented its own BYOD program, because the county started to have data management concerns. Its former provider BlackBerry would route all transactions related to data access to a central server, but as employees started bypassing the central server by bringing their own devices, such as iPhones, the county began the conversation of BYOD. iPhones posed a security concern because the IT department did not have the capacity to access, support or manage the device. In the words of chief information security officer and assistant CIO for Napa County, Gary Coverdale, “We were becoming quite concerned about security and being able to meet our compliance regulations.” Therefore, the city embraced the BYOD concept.

Napa County took into consideration various regulations from the local to the federal levels before implementing. Such regulations included the Health Insurance Portability and Accountability Act, and the State of California’s data breach disclosure law. In Napa, the county implemented a stipend program in order incentivize employees to use their own devices. The stipend program is calculated by the amount of related work activities divided by the number of total activities on the device.



BYOD

EMM

INFO  
SEC

COST

CASE  
S

REC



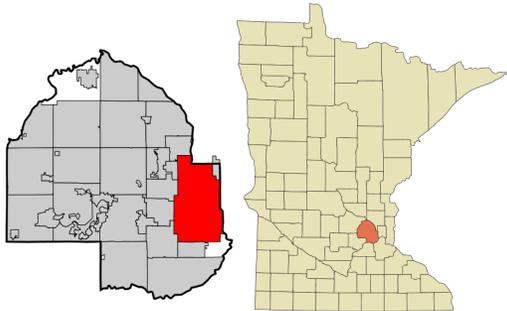
# Minneapolis, MN

In 2009, the City of Minneapolis implemented a BYOD program. Initially, the program was exclusively for smartphones and later it expanded to tablets and other devices. The City established its own internal app store for employees, which operates on iOS. This means that employees need an Apple device to access city business functions. However, employees with android and Window-based devices can access the network via the web.

The main reason the city implemented BYOD was it already had regulations and rules related to accessing city-related information from personal computers. Mainly, those protocols applied to employees that were already retrieving work-related emails from their own personal computers at home. Therefore, it was an easier transition for the city to expand access to city data on smartphones, tablets and other devices.

In the city of Minneapolis, there two types of services: basic and premiere. The basic service includes access to E-mail, Calendar, Tasks and Contacts. The premiere service includes access to all of these features, in addition to the city's network and applications.

What the City of Minneapolis observed was that BYOD did improve their worker's efficiency and productivity, especially those employees using tablets. Those employees were able to take notes and immediately access information related to decision-making processes from their tablets. Another important feature that makes the BYOD program in Minneapolis effective is their city-wide Wi-Fi. This makes it easy for employees with tablets to connect to the Internet throughout the city.



BYOD

EMM

INFO  
SEC

COST

CASE  
S

REC



# Wake County, NC

Wake County in North Carolina implemented a Bring Your Own Device program in 2012. The county divides access to sensitive information in three types of profiles depending on the seniority of the employee. The three types are minimal, moderate and full.

- Minimal: web access (on internal Wi-Fi guest network), email on web client -- no security policies or requirements at this level; uses MAC addresses to control devices on network
- Moderate: email, VPN, share drive, remote access
- Full: moderate + Lotus Notes (IBM Notes), mobile device clients, etc.



Currently, there are 150 Bring Your Own Devices that are moderate or full profiles. In addition, the county has 750 iPhones on another program called corporate owned, private enabled (COPE). AirWatch MDM manages this strategy via containerization. The county has a stipend program in place, which is handled by human resources. Employees see the stipend as a pay item on their paychecks. The stipend is \$25.00/month, which is nontaxable. The BYOD program saves the HR department about 25% to 50% in expenses. The County of Wake was formerly with Blackberry. Because employees were unsatisfied with the provider, BYOD was well received. Initially, the program piloted with senior management. The pilot program lasted 6 to 9 months; then, it was phased into the lower ranks of government.

BYOD

EMM

INFO  
SEC

COST

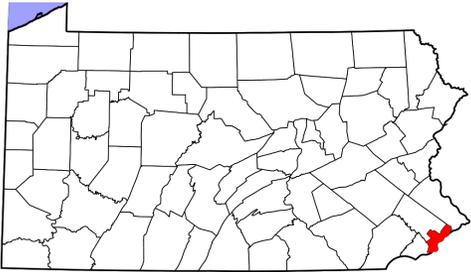
CASE  
S

REC



# School District of Philadelphia

The School District of Philadelphia is an interesting case study, because it is in same state as Pittsburgh – Pennsylvania. Pittsburgh and Philadelphia face the same federal and state laws that may impede either city from implementing certain programs. The State of Pennsylvania has one of the strongest teachers unions in the nation, ranking number #4. For organizations considering BYOD, unions are major concern.



In 2014, the School District of Philadelphia officially implemented a Bring Your Own Device (BYOD) program. Students and teachers are allowed to use their own personal mobile devices via the District's BYOD Wi-Fi wireless network for educational purposes. Of course, there are guidelines and rules on when it is appropriate for the devices to be used which the principals and teachers at individual schools determine. The program piloted with 600 students at Central High School in Philadelphia. The school district approved the program because they felt that BYOD offered students a more personalized approach to learning, which would increase productivity and results.

For more information visit: <http://www.edexcellencemedia.net/publications/2012/20121029-How-Strong-Are-US-Teacher-Unions/20121029-Union-Strength-Full-Report.pdf>

BYOD

EMM

INFO  
SEC

COST

CASE  
S

REC



# Bank of Tokyo

In 2012, the Bank of Tokyo Mitsubishi UFJ, BTMU, switched from corporate owned devices to a Bring Your Own Device (BYOD) program. However, the program was only adopted by MUFG Union Bank within the umbrella of BTMU in the United States. The bank postponed deployment of BYOD in order to further evaluate the risk and mitigates; nonetheless, it hopes to implement the program throughout the other organizations and all its global locations as soon as possible.

The primary reason the bank implemented BYOD was to reduce costs and enhance usability. Though, the bank has yet to figure out if BYOD has in fact reduced expenditure; the bank claims that BYOD has had a positive impact on the productivity of its employees. The bank does not have a stipend program for employees. Instead, the Bank pays the fees for the corporate applications that employees have access, and the users are responsible for the costs associated with the device and service plan.

In order to be part of the program, an employee must submit a written authorization stating that he or she will only use the corporate application for business activities only. If the device was to be contaminated with a virus or there were to be a data breach, the employee is required to bring the device to the device management section of the Bank. Furthermore, if an employee does not need the corporate application anymore, they must submit the device to the section as well. There, all data would be completely deleted. Also, if the device was to be either lost or stolen, users are requested to contact the helpdesk in order for them to remote wipe the device.



BYOD

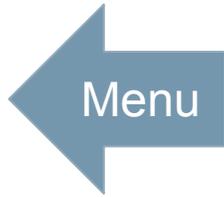
EMM

INFO  
SEC

COST

CASE  
S

REC



Recommendation

Operational Benefits

Financial Benefits



# Recommendation

BYOD is being quickly adopted across private companies, non-profit organizations, and governments across the world. As established by research findings, BYOD has advanced the workplace technologies of different organizations including governments for a cost less than their original IT expenditures.

While implementing BYOD is not the most comfortable option in comparison to the status quo, the Heinz Team asserts that it is not only viable, but that BYOD implementation would also be the best choice for the long term benefit of the City of Pittsburgh. Therefore, the Heinz Team recommends a city-wide collaborative planning process followed by a departmentally phased implementation through enterprise mobility management software to manage corporate and personal devices.

## PROS:

- Proactively addresses legal issues
- Enforced security policies via EMM
- Cost savings: devices, support, plans
- Streamline government operations
- Productivity, employees satisfaction

## CONS:

- Proactively avoid legal/privacy issues
- High initial costs, uncertain ROR
- Granularity depending on approach
- Personal device functionality
- Privacy concerns: tracking
- Lack of device standardization

BYOD

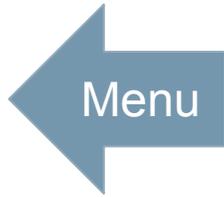
EMM

INFO  
SEC

COST

CASE  
S

REC



# Operational Benefits

Recommendation

Operational Benefits

Financial Benefits



Currently, the City of Pittsburgh spends an average of about \$500k on devices, plans, and modems. These devices consist of a mixture of smart and basic phones, making the range of technical capability for government employees inconsistent across departments. In order to uniformly advance the City of Pittsburgh IT operations, it is important that devices remain current, so that every employee device can support innovative applications that modernize government operations. Imagine the City of Pittsburgh streamlining city complaints using a Mobile311 app like the City of Riverside, CA. This application would not only allow citizens to file their complaints easily, it would also give city employees faster access to these complaints and in turn improve the overall response rate. What if the City of Pittsburgh could also give the legal community instant access to court docket calendars, fee schedules, forms, and contact information using the Attorney's Toolbox app like the City of Jefferson Parish, LA? This could reduce the call volume for the City of Pittsburgh Department of Court Records, and allow them to focus on other important functions. Supporting new apps is just one of the numerous benefits of adopting current technologies. Yet, it illustrates on a small scale how updating devices across departments would positively impact the City of Pittsburgh.

BYOD

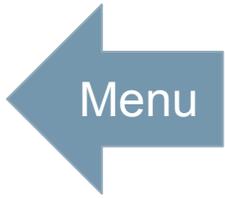
EMM

INFO  
SEC

COST

CASE  
S

REC



Recommendation

Operational Benefits

Financial Benefits



# Financial Benefits

Additionally, BYOD gives the City of Pittsburgh the opportunity to advance their IT operations while reducing their current expenditures. Many organizations that have implemented BYOD have reduced their expenses, by transferring 20% to 60% of the cost of plans and devices to the employee. The employee enjoys the benefit of a new phone for less money than it would normally cost, and the City of Pittsburgh enjoys the benefit of a more technological advanced workforce. As explained previously in the analysis, BYOD places the onus of updating devices on the employees' plan provider. Therefore, each employee would automatically receive an upgrade to the most current device every two years.

BYOD

EMM

INFO SEC

COST

CASE S

REC