CIRMA

A "Bring Your Own Device" security program helps municipalities secure access to their information systems by employees using their personal mobile devices.

Creating Your Own BYOD Program:

Risk Management for Business Use of Personal Mobile Devices

Connecticut Interlocal Risk Management Agency
545 Long Wharf Drive, 8th Floor
New Haven, Connecticut 06511
www.CIRMA.org

June 2016

If proper controls are in place, allowing employees to use their own devices for work can be a win-win.

The use of portable devices, whether personal or organization-owned, increases the risk of:

- Data loss when a physical device is lost,
- Data exposure when sensitive data is exposed to the public or a third party without consent,
- Increased exposure to network-based attacks between the network system and the device over the Internet.

An individual's smartphone can have tremendous amount of information on it – both personal and business. One's calendar, contacts, browsing history, location history, email, and more can all be (and often is) stored within the memory of the device or the device can provide an easy online gateway to all of this information.

Trendmicro.com

Mobile devices are now deeply embedded into municipal work life, improving employee productivity and communication especially during weather or other emergencies. This practice, however, creates a unique information security exposure when employees use their own personal mobile devices to conduct work. The use of personal devices is now commonplace: a recent survey found that nearly 70% of all smart phones used for business activities were owned by workers, rather than their employers. For municipalities and public schools, the practice exposes them to significant cyber security risks from devices that they do not own, directly control, or sometimes even know about.

Fortunately, software companies and cyber security organizations have stepped into the fray to develop new technology and best practices that balance the convenience of personal mobile device use with the organization's security requirements. While similar to security programs for organization-owned devices, these "Bring Your Own Device" solutions address the additional concerns of segregating personal data and applications from business data and applications on the device so that business data can be controlled, secured and monitored.

BYOD security programs typically have three major components:

- A **written policy** outlining the responsibilities of both the employer and the users.
- A **user agreement** that employees must sign, acknowledging that they have read and understand the policy and its requirements. A training component may be employed as well.
- A **software application** that will manage the mobile devices to be connected to the network.

When designed and implemented thoughtfully, BYOD programs foster productivity, mitigate risk, protect privacy, and keep proprietary information secure. They employ one of several technical strategies with differing degrees of security:

- Limited separation: Allows co-mingled corporate and personal data and/or application processing on the personal device with policies enacted to ensure minimum security controls are still satisfied.
- "Walled garden": Contains data or corporate application processing within a secure application on the device.
- Virtualization: Provides remote (and secured) access to computing resources so that no data or business application processing is stored or conducted on the personal device itself.

Begin by understanding your risk tolerance

Understanding your organization's risk tolerance is the first step to developing a successful BYOD program. Municipal governments and public schools are typically more risk averse than private sector companies. A BYOD Risk Tolerance Assessment will help identify areas of concern or focus for your organization. Consider performing a SWOT analysis as part of the assessment—as well as a survey of actual devices being used. The information will provide you better understanding of your organization's usage demands, tolerance for risk, demands on IT, and what specific issues the program must address. At this point, you should have a basic understanding of the goals of your stakeholders and the program itself.

Creating your BYOD Policy

In general, your policy should define what types of organizational resources can be accessed via mobile devices, what types of mobile devices are permitted, degrees of access, and how provisioning should be handled. Some specific issues that leaders may also consider when developing the policy include:

- The users—are they tech savvy? Frequently on the road?

"A fully featured Mobile Device Management suite actually encompasses a lot more than just device management, although that remains the starting point for an end-to-end solution. The other layers that need addressing are the applications running on the devices, the network connection to the enterprise and the data that's accessed, shared or generated. The term that captures this expanded functionality is Enterprise Mobility Management (EMM), and many MDM vendors are busily extending their products in this direction."

Charles McLellan,
Consumerization, BYOD and MDM: What You Need to Know

- FOIA, HIPPA, and other legal requirements,
- Ensuring compliance with Fair Labor Standards Act (FLSA) (overtime requirements); implications for equal rights employment practices (e.g., disparity in quality of personal devices).
- Acceptable uses of the devices, including use of cameras, personal use during business hours, business ethics considerations, etc.
- Liability to employees for lost devices, data.
- IT support capability and load implications of an increased number of devices accessing the network.
- What types of devices will be allowed—how often will this list be updated?
- Security procedures and requirements for the devices—specifically, password protocol, user profile, installation of other apps, "wiping" policy.
- Authorization process—including review of device by IT and signing of User Agreement.
- Decommissioning (wiping) devices that are lost, stolen, replaced or when employment is terminated.
- Reimbursement, if any.

Once created and published, your BYOD policy will provide your employees with clear guidelines for using their personal devices at work. In addition, it will give your IT department the authority to manage these devices against the same standards as town- or school-owned devices. Once your policy is developed, the User Agreement can be written and training provided. In general, the User Agreement (and any training) should contain statements regarding:

- Definition of acceptable uses and privacy statement
- Any risks assumed by users and liability disclaimers, if any.
- Notice of FOIA/legal discovery issues.
- What to do if a device is lost or stolen/how to safeguard personal data.
- Disciplinary actions for non-compliance with requirements.

The Mobile Device Management (MDM) Software Application

The third component of a Mobile Device Management program is the MDM application itself. A number of software vendors have developed a range of sophisticated, scalable solutions over the past several years. These MDM applications streamline the data control and device management process while facilitating employee productivity. Typically, they consist of:

- Mobile device-side apps that allow access to the organization's intranet, networks, documents, and information ensuring personal and business applications and data are segregated.
- IT products that allow IT to set policies (user profiles) for clients, manage and monitor data security, locations, and activity remotely.

Tech security experts recommend, at a minimum, that the MDM solution must require users to set and renew passwords, business data to be encrypted, and remote locking and wiping of lost or stolen devices. Other important functionality includes auditing (of device features, status and usage), location tracking, hardware management (disabling a device's camera or Bluetooth connectivity where necessary, for example) and synchronisation (for integrating mobile device policies with existing IT management infrastructure). And of course, the MDM solution must support your organization's native applications, platforms, and devices.

Examples of what an MDM solution can and can't "see" on an IOS Device:

MDM can see:
Device name
Phone number
Serial number
Model name and number
Capacity and space available
iOS version number
Installed apps

MDM can't see:
Personal mail, calendars, contacts
SMS or "i-messages"
Safari browser history
FaceTime or phone call logs
Personal reminders and notes
Frequency of application use
Device locations

Apple.com

For additional information on this topic, please contact your CIRMA Risk Management Consultant.

Although the MDM solution segregates personal and business data and applications, the MDM solution must still monitor and manage other personal applications on the device to prevent, for example, a rogue downloaded program from compromising the network. Therefore, MDM suites should provide IT managers with an inventory of all the apps running on users' mobile devices and, ideally, accommodate a customized enterprise app store where approved apps can be made available securely. Apps that are insecure or damaging in some way to employee productivity may be blacklisted as well.

A more advanced feature is app-specific security through "containerisation" (known as "app-wrapping"), in which important apps such as corporate e-mail get individual secure connections to the enterprise network. The solution should integrate with your existing network security infrastructure, so that it can monitor device usage and maintain control over access to the network, preventing unknown, unauthorized, or "jailbroken" devices and rogue apps from entry.

With an MDM solution in place, town and school district IT administrators can securely enroll devices in an enterprise environment, configure and update settings, monitor compliance with municipal policies, and remotely wipe or lock managed devices, thus enabling secure access to town and school data and applications—regardless of who owns the devices.

Before you select or implement an MDM:

- Consider the merits and fit of each vendor's solution with your needs.
- Conduct a pilot test of the mobile device solution.
- Implement the program on all devices that have access to your systems.
- Periodically assess your mobile device policies and procedures.

Additional Resources:

www.whitehouse.gov/digitalgov/bring-your-own-device. *Guidelines and case studies.*

www.itmanagerdaily.com/byod-policy-template. *Sample policy statement.*

www.shrm.org/templatestools/samples/policies/pages/bringyourowndevicepolicy.aspx. *Sample policy.*

http://www.zdnet.com/article/consumerization-byod-and-mdm-what-you-need-to-know/3/ *Vendor ranking.*

https://cio.gov/wp-content/uploads/downloads/2013/05/Federal-Mobile-Security-Baseline.pdf

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf. *Comprehensive guidelines for managing mobile devices.*

The Connecticut Interlocal Risk Management Agency, CIRMA, is Connecticut's leading provider of municipal risk financing and risk management services. A member-owned and governed agency, CIRMA provides high quality insurance for municipalities, school districts, and local public agencies. CIRMA operates two risk pools, the Workers' Compensation and the Liability-Auto-Property pool. It also provides Heart & Hypertension claims services and claims administration and risk management services to self-insured municipalities. CIRMA's financial strength enables it to provide assured rate stability, open availability, and expert risk management and claims services.

Bring Your Own BYOD Program: Risk Management for Business Use of Personal Mobile Devices