

## INTRODUCTION

iPhones, iPads, Android-powered devices, and Windows phones have grown into powerful computing platforms, and their use allows enterprise employees to connect to work as never before. These devices offer greater flexibility and adaptability — whether it's for business or private use. Ideally, consumer devices can extend and supplement enterprise desktop and laptop machines, allowing employees to remain connected to the enterprise without being chained to a physical office. Incorporating consumer technology into a corporate IT system requires planning, policy, protection, and control.

## BENEFITS

Allowing employees to use their private devices for business purposes relieves employees of the burden of carrying two devices, one for personal use, one for business. Having only one device for all purposes means that the employee is also more likely to carry the device regularly, maximizing its potential business utility.

An employee may be more satisfied (and, as a result, more productive) if they are allowed to use their favorite device rather than one forced upon them by their employer. Employees will also, naturally, have a greater incentive to protect their device from theft or loss if they actually own it.

Beyond devices, in the world of consumer applications, Facebook and other social networks have become a critical component of many enterprise's marketing strategy. Other companies have found it profitable to make use of third-party cloud services for such functions as e-mail, video-conferencing, file hosting and sharing, archiving, and order fulfillment. These applications can be particularly useful to smaller enterprises who lack the resources to develop such applications in-house or license them from more traditional vendors.

Employees have also found it convenient to carry knowledge and expertise gained from private use of these applications over to use of them in a business context. If a worker can use the same applications and services for both work and pleasure, he is freed from the need to become familiar with two sets of tools with overlapping utility.

And the benefits to the IT department include cost avoidance for device purchase, and a technology adaption process that keeps pace with innovation.

## OPTIONS IN RESPONSE TO CONSUMERIZATION

There are three basic options for an enterprise in deciding how to incorporate consumer devices and applications in the business world.

- 1.) The enterprise may allow employees to freely choose the devices and applications they use for work purposes, through an unrestricted BYOD program.
- 2.) The enterprise may restrict employees to using only company-issued devices for business purposes. Personal devices are completely excluded.
- 3.) The enterprise may create a list of approved devices and provide support for them. Corporate or personal owned depending on user type and policy.

### Trend Micro™ Mobile Security

- Alleviates IT burden by providing visibility and control through an integrated mobile device management and security solution
- Protects devices, data and corporate infrastructure
- Manages mobile applications
- Lowers the cost of supporting mobile users within a BYOD environment

All within an integrated management framework that manages the security of PCs and mobile devices from a single console.

The first option, obviously, is fraught with peril from a security standpoint. An insecure device with network access privileges can become a serious vulnerability, potentially compromising the enterprise network and making all its data vulnerable to unauthorized usage and attack. There are also difficulties with ensuring that enterprise applications, including e-mail and VPN clients, are usable on all devices, and the additional help desk costs that may result. Additionally, many of the applications available to employees in this model are likely to have serious security or liability issues of their own, and in an open model it is difficult (if not impossible) to stay abreast of all concerns.

The second option, though attractive from a security standpoint because it allows total control over devices used for business, fails to capture any of the consumerization benefits described above. Enterprise employees will tend to regard such a policy as insular and reactionary, and may resent the imposition of company devices, which they may find clumsy and outdated compared to their personal devices.

The third option is a hybrid approach between the two others, allowing some flexibility in an employee's choice of tools without opening the field to devices whose integrity the company may have reason to doubt. Ideally, the most popular devices and applications can be cleared for use, satisfying the majority of enterprise employees. If a popular device or application is disallowed, the reasons for that decision can be clearly communicated to employees, potentially mitigating any resulting dissatisfaction.

You may wish to issue some users a corporate-owned device, but give them a choice of options. This is more important for heavy users where the personal call and data rates are not as good as the organization's, especially for international travelers. You may even decide they can bring their own device but the company takes over the airtime and data costs. The key here is to group users by usage and build a flexible policy which works best for all groups as well as the organization.

### STANDARDS, COMPLIANCE, AND REGIONAL DIFFERENCES

Any device using the corporate network, whether it is personal or company property, must remain properly certified for network access. Processes must be put into place to revoke certification if the device becomes compromised, if the employee uses it in a way that violates organizational policy, or should they leave the organization.

For a BYOD program, employee compliance should be a pre-requisite for participation in the program. If an employee wishes to use their personal device for work, they must also be willing to be an active partner in ensuring the device's security. If the device's certification must be revoked, the reasons for this action should be clearly communicated to the employee, and an opportunity for self-remediation of the security violation offered.

### CHECK LIST FOR CREATING A BYOD POLICY

Follow these steps to create and maintain an effective policy for consumerization.

- Convene a policy committee with representation from IT, Human Resources, Executives, Power Users, IT support, and the Legal department
- Determine which of the above models will be used; Strict, Open, or a Balanced policy
- Segment users based on their need for access to corporate data and applications
- Survey which devices are already being used by employees
- Make a technology decision for MDM (Mobile Device Management), DP (Data Protection), Mobile Security and Mobile application management
- Determine what actions will be taken when an employee's device is lost, stolen, or replaced and when an employee leaves the organization
- Publish policy and get employee acknowledgement
- Deploy controls to enforce policy
- Refine policy as technology, threats, and environment changes

## SECURITY AND THREAT CONCERNS

The primary risk from mobile devices is the danger that an enrolled device may be lost or stolen, endangering the security of enterprise data and applications. Even if a business-use device remains safely in the employee's hands, an employee may be careless with what applications they run or what security measures they put in place on his own personal property.

Consumer applications will require vetting and blacklisting if they pose a threat. Organizations should be careful how much they entrust to web and cloud applications whose internal functions they have little control over, and should implement policies to avoid passing or storing sensitive or private information over or within these applications.

Malware is starting to show up that targets mobile devices. Companies should also ensure that even personal devices have some corporate centralized management utility to enforce passwords, limit application usage, etc., and that employees are informed as part of the policy sign up process.

Mobile devices have become targeted by adversaries as vectors of attack, especially for executives traveling abroad. If an attacker can gain physical access to the mobile device they can offload data and install custom malware. The strongest possible controls are required to protect these devices. In addition to data theft, features of the phone such as voice and video recording or sending and dialing premium rate SMS and phone numbers for profit could be exploited.

## PROTECTING USERS, DEVICES, AND DATA

Best practices for implementing effective and secure consumerization include:

- 1.) Maintain and regularly update a registry of risky apps or programs which cannot be used on devices connect to the enterprise network (mobile or desktop). This registry should be open for viewing by any employees participating in a BYOD program, or using their personal machines for work purposes. You can also enforce this through an enterprise MDM solution like Trend Micro's Mobile Security solutions that include Mobile Application control on top of traditional mobile device management capabilities.
- 2.) Encourage quick reporting of lost or stolen devices, and respond proactively with a remote lock or wipe. Always ensure passwords are enforced on the device.
- 3.) Implement the ability to perform selective wipes that will only target corporate data stored on a private device. Caution must be exercised to avoid antagonizing an employee by wiping his/her personal data.
- 4.) Enforce authentication for personal devices and apply proper encryption to enterprise data.

- 5.) Seek legal advice to determine organizational liability for an employee's usage of his own device, or for use of a third-party web application, and set policies accordingly. This will also need to include how you treat their personal data applications, especially when it is an employee-owned device.

Caution and clear-thinking are necessary to avoid over regulating a consumerization/BYOD program into uselessness. A policy that makes it prohibitively difficult for employees to use consumer devices and apps will, ultimately, have results indistinguishable from those of a "company devices only" policy. At the same time, sound judgment is needed to avoid exposing the network and the organization's proprietary data to attacks, corporate espionage, and harmful disclosures. We must remember the reason employees are putting pressure on businesses to embrace these consumer devices and applications. They want to use technology they understand and that makes their life better. If we over complicate things they will just find other devices or technology to achieve their goal.

## REFERENCES

Consumerization. The power of many: The shift from personal to personalized computing. The Economist (Oct. 8, 2011) <http://www.economist.com/node/21530921>

David Moschella, Doug Neal, et al Consumerization of Information Technology. Leading Edge Forum, 2004, <http://lef.csc.com/projects/70>

[www.trendmicro.com/mobilesecurity](http://www.trendmicro.com/mobilesecurity)