spectrum inc
COMMUNICATIONS SIMPLIFIED

WHITE PAPER

BYOD or COPE — Which Is the Better Option for Your Organization?

EXECUTIVE SUMMARY

In the midst of the mobile device revolution, companies were forced to devise strategies to manage associated equipment and wireless carrier costs. Out of necessity, companies had to quickly adapt to the influx of wireless devices in the workplace. Two common wireless management models in use today are "bring your own device" (BYOD) and "corporate owned personally enabled" (COPE). Each has its own pros and cons, and a thorough understanding is required to decide which is the better option for your organization.

An Increasingly Mobile Workplace Introduces Wireless Management Challenges

It wasn't too long ago that the BlackBerry was among the few wireless handheld devices found in the workplace. For its time, this innovative productivity tool was reserved for the select few for whom persistent access to email and connectivity were deemed mandatory for conducting business. And through the first half of the 2000s, those executives, power players, and technologically inclined individuals were the exception, as the majority of the workplace remained largely land-locked.

Then, a wireless revolution occurred. The iPhone was released in the summer of 2007, followed by an influx of Android-based phones later that year. During this time, mobile adoption among the workforce started to become commonplace, and the wireless-enabled lifestyle began to appeal to the population at large for its educational, recreational and social purposes. Today, 90 percent of American adults have a cell phone, while 58 percent own a smartphone. [1]

This revolution meant that employees at all levels were incorporating smartphones to stay connected to company networks and increase productivity. As time went on, other wireless and mobile computing devices, such as tablets, laptops and tablet-laptop hybrids were added to the wireless mix.

The task of managing the costs associated with how these devices were used to perform daily business operations was thrust upon companies, whether they wanted to deal with it or not. Most companies were not prepared to manage this responsibility and were forced to quickly adapt.

Initially, most companies sought to control network security and device compliance by adopting a wireless management model that severely limited the number of devices its employees could use. This method, known as corporate liable, also revealed the difficulties many companies encounter with the internal administration of wireless management policies. With more devices entering the workplace, these management challenges became even more pronounced. As a result, many companies abandoned corporate liable in favor of a simpler approach.

Today, many companies are moving toward two wireless device management methods that evolved from the corporate liable model:

- **BYOD: Bring Your Own Device (individual liable) —** seen as an attractive alternative to corporate liable, BYOD places the responsibility on each employee to select and bring their own device to perform work-related activities
- **COPE: Corporate Owned Personally Enabled —** a recently adopted approach that places control back into the company's purview while providing employees with the option to select the mobile device of their choosing

The purpose of this white paper is to explore the pros and cons of each approach and help you determine which wireless management method is better for your company.

BYOD: Easy to Implement, Not as Easy to Support

By nature of its implementation simplicity, BYOD has become widely adopted by many companies as the path of least resistance for wireless management. Companies are willing to let employees absorb wireless device acquisition and management to avoid equipment costs and the expense of internal administration. From this point of view, BYOD's upside is fairly evident:

- **Increased employee morale —** employee chooses their own device
- **Ease of implementation —** device purchase and carrier costs are absorbed by the end user; little to no strain on IT department for maintenance and upkeep
- **Increased productivity —** employee gains access to email and network data

BYOD, however, is not without its problems. In the haste to establish a wireless management policy, many companies forgo careful investigation of BYOD's pitfalls. Those same companies have since discovered that there are several unintended expenses and challenges associated with BYOD:

- **Stipend —** fixed monthly usage/data "allowance" for each employee with a device; doesn't always cover all business-related usage (e.g., international roaming charges)
- **Security risks —** lost or stolen phones represent the potential for unwanted access to sensitive company data and its larger network; increased potential for the introduction of malware to access/infect the company's network
- **Mobile Device Management (MDM) services —** need for third party vendor and/or software that controls data and configuration settings for in-network devices; maintains separation of corporate and personal information; drives usage policy compliance across employee devices; and helps to maintain device security

- **Unplanned IT management —** internal department is often taxed with unplanned support and management of wireless/connectivity/security issues, including: implementation of MDM; management of wide variety of devices; responding to potential security issues
- **Loss of visibility —** wireless expenditures are largely unknown
- **No corporate buying power —** individual is unable to benefit from corporate leverage
- **Lack of helpdesk —** is there a helpdesk or support resource prepared to deal with the influx of inquiries from employees using multiple devices?

In addition, companies often see escalating expense reports from employees who include device repair and replacement into monthly expenses. While on the surface BYOD seems like a low-maintenance, cost-cutting approach, on closer inspection, the costs of BYOD begin to quickly add up.

COPE Provides a Secure Alternative

In light of BYOD's inherent unpredictability, COPE is emerging as a viable alternative, giving companies a way to reign in unforeseen wireless expenditures and reduce security nightmares. The COPE model adopts the personal device selection aspect of BYOD and brings with it the many benefits of corporate ownership. In many ways, COPE could be considered the best of both worlds. However, it does require a much more formalized strategy to implement successfully.

With COPE, the responsibility of wireless management falls on the organization or a trusted wireless management partner. In most instances, the company's IT department creates a preferred list of available devices from which employees can select. These devices are then managed according to the company's network security policies and safeguarded more effectively from a central location — rather than individually by the employee. Many companies also employ MDM services to assist with driving compliance and monitoring device security throughout the organization. All equipment, management, MDM services and carrier costs are absorbed by the company. COPE eliminates many of the risks inherent to BYOD and provides many additional benefits:

- **Corporate purchasing —** leverages the power and advantages of a corporation to negotiate discounts on equipment and contracts, and manage device upgrades internally
- **Limit unexpected usage costs (roaming, etc.) —** usage/data plans are devised to control costs and account for employee-specific job responsibilities (international travel, etc.)
- **Employee benefits —** access to IT and helpdesk support; device replacement and updates managed by IT or a trusted wireless management partner
- **Mitigate security risks —** enables safeguards to protect corporate assets
- **Mobile Device Management (MDM) services —** like BYOD, third party vendor and/or software is needed to control data and configuration settings for in-network devices; maintain separation of corporate and personal information; drive usage policy compliance across employee devices; and help maintain security
- **Internal IT and helpdesk support —** provides improved ability to manage and control devices, maintain compliance with app updates as needed

Combining the flexibility of BYOD with the advantages of corporate ownership, COPE is a win-win for companies and employees alike. See Figure 1 for a snapshot of the pros and cons of each wireless management method.

Figure 1: Comparison of BYOD and COPE for employees and organizations

Wireless Management Model	Employee		Company	
	Pros	Cons	Pros	Cons
BYOD	Selects device of his/her choice	Absorbs equipment and carrier costs Limited device support from employer (IT and helpdesk)	No investment in equipment or carrier costs	Pays monthly stipend to employees More risk for security issues Requires MDM services to successfully manage Unplanned IT management Lack of helpdesk to support employee issues
COPE	Selects device of his/her choice Not responsible for equipment or carrier costs Access to support from employer's IT and helpdesk	Must select from pre-approved company devices	Internally managed: IT department controls and manages devices; helpdesk provides ongoing support Mitigates security risks Leverages corporate purchasing Limits unexpected costs Controls device upgrades and app updates internally Drives compliance across all devices in the organization	Absorbs equipment and carrier costs internally Internal resources required to manage Requires MDM services to successfully manage

Conclusion: COPE Is a Sound Investment in the Future

If driving compliance across the organization and reducing security risks are important to your organization, then COPE is probably the best fit for you. COPE requires an up-front investment and ongoing efforts to manage a formal in-house wireless management program. But, when implemented properly, it's an investment that can pay dividends to the company's bottom line and protect its operational security.

On the other hand, BYOD represents a more laissez-faire approach to wireless management. But this freedom comes with a price, including: a loss of visibility to wireless expenditures; increased security risks; and a lack of device control and compliance across the organization. Ultimately, the decision to choose BYOD or COPE depends on your company's willingness to implement its own internal mobile device management policy and accept ongoing administration responsibilities. While BYOD continues to provide some companies with a small measure of wireless management success, its widespread adoption is becoming a thing of the past.

For complete wireless cost optimization, including MDM services, helpdesk and implementation support of BYOD or COPE, please call the experts at Spectrum, Inc. at 513-697-2000.

References:

1. http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/