WHITEPAPER

BALANCE END USER SATISFACTION AND BUSINESS PRODUCTIVITY

Making the case for COPE
A flexible, secure alternative to BYOD

BlackBerry

iOS

MAKING THE CASE FOR COPE

Contents

The steady adoption of Bring Your Own Device (BYOD) and Application (BYOA) polices, two of the major catalysts in the consumerization of IT movement, is the source of both widespread optimism and angst inside thousands of enterprises and organizations. Executives and line of business managers foresee business-altering productivity and profitability gains resulting from a mobilized workforce fully empowered to work from any location and at any time using the computing and communications tools of their choice. CIOs and IT administrators, though fully embracing the same productivity goals, harbor significant concerns that the rampant infiltration of consumer-oriented devices and applications into the corporate workflow will lead to potentially catastrophic losses of sensitive information, render corporate data vulnerable to malicious attacks and expose businesses and executives to costly legal or reputation-ruining actions related to privacy or compliance violations.

The good news for LOB leaders and CIOs alike is that recent advances in enterprise mobility management (EMM) and rising concerns over the long-term security implications of unfettered BYOD and BYOA is providing fresh momentum for an enterprise mobility approach known by the acronym COPE, or Corporate Owned, Personally Enabled. Occupying the territory on the mobile device policy spectrum between Corporate Owned, Business Only (COBO) and BYOD options, COPE provides IT departments with a rich set of levers and knobs to pull and twist in the never-ending and all-important quest to balance end-user satisfaction and business productivity with enterprise security.

△ Back to the Contents

Introduction

BYOD /b-y-o-d/ *noun 1. Bring Your Own Device*. An enterprise mobility device management approach characterized by workers using personal devices, namely smartphones and tablets, to conduct work-related computing and communications activities.

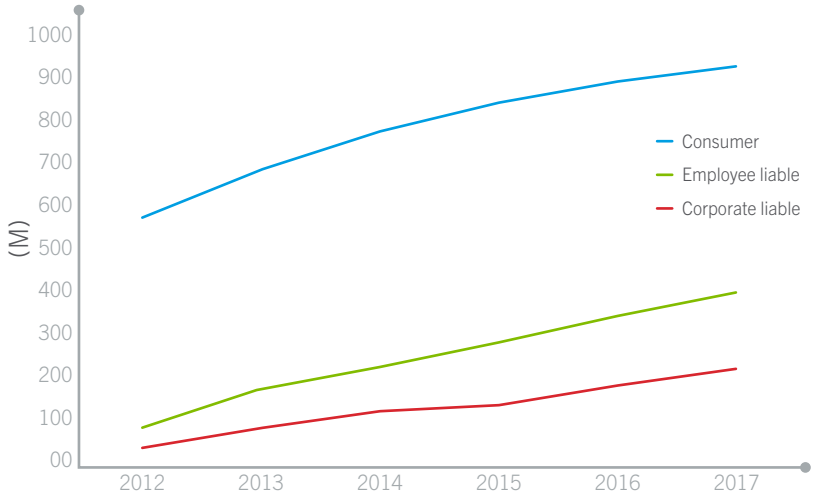
COBO /köbö/ *noun 1. Corporate-Owned, Business Only*. An enterprise mobility device management approach characterized by a business or organization issuing employees a mobile device that is dedicated to work-related computing and communications activities.

COPE /köp/ *noun 1. Corporate-Owned, Personally Enabled*. An enterprise mobility device management approach characterized by a business or organization offering employees a choice of smartphones or tablets that are owned by the business but configured to allow personal computing and communications activities by employees.

Enterprise mobility is a runaway train. Businesses, witness to just a sampling of the transformative effects of providing workers with the ability to do their jobs outside of the office and normal business hours, are poised to accelerate enterprise mobilization over the next few years. Business unit managers are licking their chops in anticipation of a salesperson, for example, empowered to give demos, check inventories and place orders in the field from a tablet or smartphone. With workers doing business in the moment, rather than being required to finalize transactions after returning to the office to tap into core business processes accessible only from inside the enterprise, business leaders hope to significantly expand productivity and profitability.

Corporate-Owned Smartphones on the Rise

Worldwide Smartphone Shipment by User Type, 2012-2017



The number of corporate-owned smartphones is projected to increase at a rate faster than the overall smartphone market, despite predictions that businesses will eventually supplant corporate-liable policies with BYOD. IDC Research estimates that of the 722.5M global smartphone shipments in 2103, 90M devices (9.4% of the total market) were purchased for corporate use. In 2017, corporate-issued smartphone shipments will grow to 234M (15% of the overall market), according to IDC.

Source: IDC, June 2013

△ Back to the Contents

If enterprise mobility is a train, the locomotive providing its propulsion is the consumerization of the enterprise, an Internet- and mobile broadband-enabled phenomenon that is synonymous with Bring Your Own Device (BYOD) polices being embraced by many organizations and businesses. The "Bring Your Own" movement, which has expanded to include applications (BYOA), surfaced roughly seven years ago and has been picking up steam ever since. The market research firm Gartner Inc., in fact, predicted in 2013 that by 2017 roughly half of all employers will require their employees to supply their own devices.

The BYOD movement is well documented and its attractiveness to business leaders is not difficult to fathom. For many organizations, embracing BYOD polices creates an energized workforce that is tapping into the latest Internet and consumer electronics innovations to do their jobs from any location and at any hour. With some employees paying for devices and even monthly voice and data plans, many enterprises also view BYOD as a mechanism for trimming capital and operational costs. From productivity and budgetary perspectives, BYOD appears to be a win-win.

The swiftness at which the mobilization of the enterprise is evolving, however, means a steady fluctuation in the variables and conditions that figure into the effectiveness and viability of a mobile enterprise strategy. Recent advancements in the EMM space and plans by many enterprises and organizations to accelerate the mobilization of core business processes, for example, are prompting some businesses to consider alternatives to unfettered BYOD policies for their mobile device strategies.

Some market research firms are predicting that businesses will begin to move away from BYOD. "BYOD prevails in many countries but corporate purchasing will experience a resurgence as companies better realize BYOD's management challenges," offered Strategy Analytics, an international research firm, in a report published at the end of 2013. "Security concerns will lead enterprises to pivot from Bring Your Own Device (BYOD) to let employees choose their own device in some mature markets." [1].

The unattractive flipside of BYOD has always been the strain it places on enterprise IT departments related to risk management. BYOD has unleashed a torrent of new devices and applications, all desiring access to closely guarded company information, into the corporate environment. Often understaffed and overwhelmed, IT departments have at times been forced to contain the flood of endpoints and apps with severe restrictions or onerous security hoops for end users to jump through in order to safeguard intellectual property. These sometimes-draconian policies, along with the fear of losing personal data or invasions of privacy, prompt many end users to avoid IT oversight, further hampering the security objectives of the enterprise.

While these conditions have made for a tenuous situation for IT administrators, many have been able to deal with the BYOD-induced management and security strain to this point by striking a viable, if not optimal, balance between security, end user satisfaction and business enablement. As previously cited, though, the quickly maturing enterprise mobility movement is influenced by several evolving variables and conditions that will likely make it increasingly difficult for IT departments operating under a BYOD-heavy approach to secure corporate environments without inhibiting the productivity advances that workforce mobilization promises.

1 Enterprise Mobility Predictions, 2014

△ Back to the Contents

So what are the coming changes in the enterprise mobility space impacting the efficacy of BYOD? The most immediate source of pressure will be a sizeable expansion and acceleration of workforce mobilization. If they are not already, CIOs soon will be confronted with the challenge of securing corporate data in environments where workers will be attaching more and a greater diversity of devices to the corporate network, mobile access capabilities will be extended to a larger proportion of the workforce and business units will mobilize additional mission-critical work processes. More devices, more users and more exposure of sensitive corporate data mean more vulnerability to data leakage or security breaches through mobile devices.

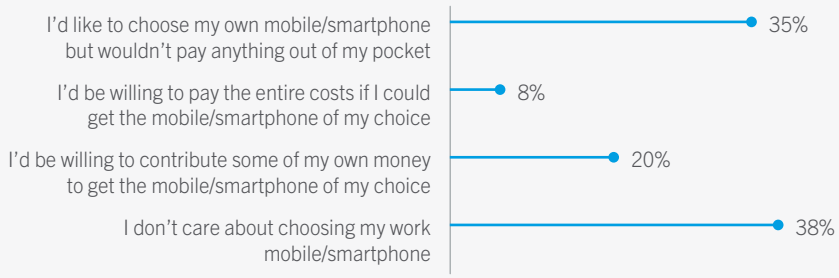
BYOD: Built for the Future?

The BYOD bandwagon has been picking up steam for the past few years. But as the mobilization of the modern workforce reaches a new phase in its evolution, becoming increasingly integral to the competitiveness and profitability of enterprises and organizations, information is surfacing to suggest that BYOD, at least in its most loosely enforced form, poses security and legal risks that may be too severe and significant for IT to remedy without nullifying BYOD's biggest benefit: user satisfaction that promotes employee productivity.

As organizations embrace mobility and enable additional users and partners to access increasingly sensitive and strategically valuable information from mobile devices, the opportunity for data leakage or attacks, as well as the associated consequences, increases exponentially. As the stakes around mobile security and business productivity continue to grow higher, the potential increases that CIOs and IT managers at security conscious organizations may be hesitant to fully embrace BYOD as the basis of an enterprise mobility strategy.

Even the long-held view that a substantial percentage of the workforce would be willing to assume the expense of acquiring a preferred personal device for work-related tasks may lack validity. A 2013 Forrester Research study, which surveyed more than 3,000 information workers in Europe and North America, found that while 35% of respondents said they would like to choose their own smartphone for work, they would not be willing to contribute anything to the cost. Only 8% said they would pay the entire cost, while 20% indicated a willingness to contribute an unspecified amount to the purchase, according to the survey. Responses to a similar question about tablets yielded results within a few percentage points of the smartphone question. The survey results suggest that a COPE-based mobility management approach, which typically provides employees with a choice of corporate-owned devices, has the potential to be at least as appealing to end users as BYOD.

"What level of interest do you have in being allowed to bring your own mobile/smartphone as your work mobile/smsmartphone?"



Source: Forrsights Telecom and Mobility Workforce Survey, Q2 2013, Forrester Research, Inc.

As enterprise mobility evolves and its adoption accelerates, additional shortcomings of BYOD may be exposed in the future.

- Management complexity. BYOD adds complexity to multiple elements of an enterprise mobility management solution, including device and application management, application lifecycle management, and telecom expense plan management. The larger the diversity of devices and platforms that access corporate data, the greater the strain on IT. According to a 2013 survey conducted by Gartner Inc., 81% of organizations reported that mobility has increased helpdesk workload. The influx of additional user devices would likely place additional stress on corporate helpdesks[1].
- Security threats are increasing. Mobile devices are being increasingly targeted by hackers and other malicious-minded individuals as entryways into corporate data stores. Like Willie Sutton, cybercriminals go where the money is and as enterprises extend the reaches of their networks across mobile boundaries, IT managers can expect mobile devices to be an increasingly attractive target for cybercriminals.
- Consumer legacy. As corporations open up mobile conduits to increasingly sensitive corporate data, more and more information is stored on consumer-oriented and consumer-controlled mobile devices, which were not designed for secure environments.
- Litigation Exposure. Though laws vary from country to country, corporations are in general better protected against legal actions from employees over privacy violations or lost information if the organization owns the mobile device, making it easier to impose policies that reduce the risk of litigation. See the sidebar "Mobility Litigation Case Files" for examples of mobile-device-related litigation and how privacy and labor laws vary from country to country.
- Added Expense. For companies that reimburse employees for mobile data and voice services or offer a monthly stipend, a BYOD policy blocks businesses from taking advantages of discounts associated with volume purchasing or the pooling of voice and data usage.

1 "The Impact of Mobility on the IT Service Desk" Gartner July 2013

△ Back to the Contents

In addition to repelling security threats in this highly mobilized environment, CIOs will also need to summon additional vigilance in guarding against legal issues related to regulatory compliance or invasion of employee/customer privacy, a task that will require strict governance of applications and content residing on mobile devices utilized for business purposes. CIOs working for multinational businesses face additional challenges, as privacy laws and cultures tend to differ across geographies. As the demands on IT departments reach new levels of complexity, CIOs are likely to closely evaluate whether the usability and business enablement benefits of BYOD can be realized without exposing the enterprise to unacceptable risks.

In search of a BYOD complement or alterative, businesses and organizations are likely to take a fresh look at the enterprise mobility model known as Corporate Owned, Personally Enabled, or COPE, a concept that took root a few years ago as a sort of compromise approach to the adoption of a strictly administered, or locked down, corporate model known as COBO (Corporate Owned, Business Only) or unfettered BYOD.

The remainder of this document takes a close look at the COPE enterprise mobility model, contrasting it with BYOD and COBO approaches, as well as detailing a few of the technology and market developments that are prompting CIOs to start kicking the tires of a device management policy with the potential to satisfy the desires of end users and business leaders, while bringing peace of mind to the IT department.

The (Hidden) Costs of BYOD

Budget trimming is often cited as an attractive attribute of BYOD. The logic supporting that proposition is that organizations can save money if employees are picking up the tab for mobile devices. While the logic behind that theory is understandable, it could be based on false assumptions and, perhaps, some wishful thinking.

Much of the true cost of BYOD depends, of course, on the nature of the BYOD policy. Even if businesses are not paying for employees' phones, chances are they are absorbing all or a portion of monthly voice and data plans through a reimbursement program, which can be significantly more expensive than the device. Corporations can realize sometimes significant reductions by purchasing large pools of data and voice minutes. Those savings are not available to organizations that pay for monthly mobile service charges on a reimbursement basis.

In addition, a wide-open BYOD policy, which will need to support potentially dozens of different devices, operating systems and versions of operating systems, could introduce management complexity that far exceeds device and application management costs associated with a more-controlled number of end user devices. Keeping track of additional devices and platforms may mean a larger technical support staff or the added expense of installing additional MDM or EMM products to cover the entire spectrum of user smartphones and tablets.

It's the unexpected costs that may result from potential security lapses associated with BYOD, however, that could end up being the most severe. Though no organization is ever completely protected from the leakage or theft of corporate data or intellectual property, the level of protection delivered by a more conservative mobile device policy is often higher than what can be reasonably expected in a BYOD environment. While it's nearly impossible to put a price tag on the loss of IP, leakage of tightly-held secrets to a competitor could have catastrophic ramifications.

Another unexpected BYOD bill could come due in the form of legal costs. Though their severity varies from country to country, the financial penalties associated with compliance or regulatory-related violations often fall into the six-figure range. Again, while no mobile enterprise device policy is infallible, the more devices and the less oversight IT has over those devices, the greater the opportunity for content that needs to be accounted for to be lost or stolen. The same holds true for litigation around employee privacy. In some countries in Europe, for example, penalties for monitoring or deleting an employee's personal information can be severe. The number of privacy invasion legal actions and the likelihood of those actions resulting in fines both tend to decrease if the company, rather than the employee, owns the mobile device.

It's not just money on the line, either. A security breach could severely damage the reputation of a business or organization, especially one that handles sensitive customer or client information, such as a business in the financial services or healthcare industries. Employee-instigated legal actions could also be a recruitment nightmare for a business or organization.

△ Back to the Contents

COPE: The BYOD Alternative

The COPE approach to enterprise mobility is largely a counter to BYOD, which, in its rawest form, poses a nightmare for IT departments. Oft referred to as the "Wild West" of enterprise mobility, an unfettered BYOD scenario is characterized by a motivated workforce accessing corporate data through an assortment of smartphones and tablets derived from multiple versions of a handful of mobile platforms, most of which were designed for consumer environments. Lacking the resources to keep up with the diversity of devices and the rapid introduction of OS upgrades, both minor and major, IT administrators toil by day to apply a thin coat of oversight to the employee-controlled mobile agents accessing the corporate network – as well as the wide open Internet – and down antacids at night to counteract concerns that sensitive data is being leaked outside the enterprise or accessed by ill-intentioned hackers.

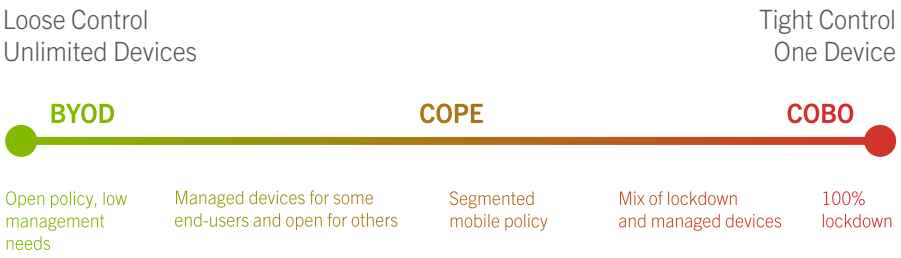
COPE is also an alternative to a COBO approach, which is often defined by ultra-conservative user polices. The organization owns the device and strictly dictates how it can be used by employees. Complete prohibition of the smartphone, tablet or rugged device for personal use is a common clause in most COBO-based user policies. It wasn't until the availability of mobile broadband, creating a high-speed pipeline between mobile devices and the riches of the Internet, that the major drawback of a COBO approach was exposed. With corporate-issued devices prohibited from use as conduits to commercial communications channels, social media sites and other Internet destinations, employees soon started to tote their own equipment into the workplace, along with desires to fuse their work and personal communications and computing activities into a single device.

Somewhere between the rigidness of COBO and the anarchy of BYOD, COPE was born. A large portion of COPE's appeal is that it supports a broad spectrum of use cases. In general, however, a COPE-governed enterprise mobility plan is one that provides end users with the ability to choose from a selection of corporate-owned and approved devices, which most likely have been pre-configured with separate work and personal environments. COPE is viewed by many IT managers as an "eat it too" proposition, as it essentially combines the control that is a hallmark of COBO with the end-user appeal of BYOD. An archetypical COPE deployment would be one that delivers unfettered productivity and superior user satisfaction, without the nausea-inducing complexity and vulnerabilities associated with loosely governed BYOD policies.

△ Back to the Contents

Though COPE is consistently portrayed in the industry as being in direct opposition to BYOD, that description fails to capture the fact that both approaches are in pursuit of the same objective: fortify workers with a mobile device that can be used securely and simultaneously for work and personal computing and communications activities. The two approaches just go about it from opposite directions. With a BYOD approach, the exercise centers on extending the use of a consumer device to the work realm. COPE, by contrast, starts from a work-first perspective, with IT carving out, or pre-configuring, a portion of the device for personal use. From a management and security perspective, it's easy to understand why COPE is increasingly viewed by CIOs as an attractive alternative to BYOD.

If corporate mobile device policies were plotted on a conservative-to-liberal spectrum, COBO polices, which in most permutations force the lockdown of smartphones, tablets and other devices for the exclusive use of corporate-approved applications and content, would be at the conservative end. BYOD polices, which in extreme instances put no limitations on the number and type of devices workers can utilize to conduct business, would fall on the opposite end of the spectrum. COPE polices can be viewed as reducing the rigidness of some COBO polices or as tightening up the loose oversight of BYOD, a perspective that pushes the two major approaches to enterprise mobility toward the center of the spectrum.



While it's an oversimplification, COPE can also be viewed as providing a flexible and adaptable set of policies that occupy the expanse of the device policy spectrum between corporate lockdown and BYOD. By enabling an amalgamation of conservative and liberal device policies, COPE is being viewed by many organizations as a mechanism for achieving the prime directive of the IT department – protecting corporate information against unauthorized access, malicious malware, and leakage, without putting business-dampening restrictions on the types of mobile devices and applications available to the mobilized workforce.

From a practical standpoint, COPE offers IT the opportunity to impose a significant level of mobile management and policy uniformity across the entire enterprise, which is typically characterized by dozens of risk profiles and use cases. Even individual workers, armed with multiple devices – controlled by a handful of OSs – can enjoy the productivity and privacy protection that COPE brings without overburdening IT with management complexity or exposing the enterprise to security risks.

△ Back to the Contents

As is the case with nearly every aspect of enterprise mobility, the tricky part of COPE policy adoption is applying the proper touch. If IT departments, for example, fail to compose an approved list of devices broad enough to meet the requirement of a vast majority of end users or issue corporate-approved applications that fall short of the usability and productivity levels of Internet-available apps, users will revert to downloading apps from commercial app stores and using their own devices for business. The ultimate aim of any COPE policy is to ensure that a large majority of users will be satisfied with their corporate-issued devices from both work and personal perspectives.

Getting COPE Correct

Given the adaptability of a COPE enterprise management approach, success or failure will depend heavily on implementation. Here's a sampling of best practice and guidelines for a COPE-based enterprise mobility architecture:

- Provide a list of approved devices that is broad enough to satisfy employees but narrow enough not to stress IT resources related to device and application management or to introduce security risks.
- Employ a containerization approach that allows for the complete separation of work and personal environments, giving workers unfettered control of the portion of the device reserved for personal use.
- Craft a mobile device policy document that clearly spells out users' responsibilities and restrictions regarding security and safety in both the work and personal environments.
- Let the business bottom-line dictate your policy toward mobile devices. Which approach – COBO, BYOD or COPE – is going to give your business the best balance of security, productivity and user satisfaction? Which approach is going to best advance your workforce mobilization initiatives?
- Don't assume device ownership is a Teflon shield against privacy invasion claims from workers. The law remains unclear in this area and while it's a safe bet that ownership provides some measure of protection in the case of wipes of personal data, IT departments should still operate with kid gloves when handling personal data.
- Don't be exclusive. Regardless of the level of flexibility in your COPE-based policies, expect a number of outliers to continue to access corporate data with personally owned devices. Extend policies to handle this inevitability and to minimize risk.
- Run it by end users. Inaccurate assumptions about the preference of end users have sunk hundreds of startups. What the IT department assumes will be acceptable and embraced by the workforce could turn out to be way off the mark.
- Strongly consider COPE for multinational deployments. Legal ramifications resulting from the deletion of employees' personal information on end points used for work vary in severity from one country to another. Company-wide adoption of a COPE-based policy will provide the best protection against lawsuits across international borders.
- One size fits all. For environments that employ a spectrum of use cases and risk profiles, as well as device and OS types, a COPE approach offers the flexibility to cover all facets of a highly stratified enterprise mobility environment without security sacrifices.

△ Back to the Contents

COPE: Why Now?

The evolution of enterprise mobility is driving a convergence of conditions that point to a positive environment for the potential wide-scale adoption of COPE-based policies. The three most prominent elements of the emerging nexus are concerns over the long-term viability of BYOD in the face of the anticipated and disruptive acceleration and expansion of workforce mobilization efforts, the maturity of application and device management technologies that enables a single device to safely intermingle work-related and personal information and the ability of COPE to allow IT administrators to impose flexible and granular enterprise mobility policies that satisfy usability and productivity needs without leaving the enterprise vulnerable to attacks, data leakage or costly legal actions.

Long-Term BYOD Concerns

BYOD is at the extreme liberal end of the corporate device policy spectrum. Classified by many as the "Wild West" of enterprise mobility management, BYOD is popular with some users and IT departments because it promotes the use of personal devices and consumer applications for the completion of work-related activities. Workers are presumably more productive using familiar tools, as well as more likely to work extended hours. BYOD has also been tagged as "IT friendly" by multiple sources for its ability to reduce both Capex and Opex, the latter by relieving IT staff from some or all mobile device management chores.

As BYOD matures and expands in the enterprise, however, information is surfacing to suggest that BYOD, at least in its most-loosely enforced form, poses significant management challenges, security and legal risks and may not be as budget friendly as once believed, prompting some businesses to seek a more-controlled alternative. See the sidebar "BYOD: Built for the Future?" for a detailed discussion of potential management and security shortcomings associated with BYOD mobile device polices.

△ Back to the Contents

Work/Life Isolation

The introduction of containerization, or dual personas, which enable businesses to isolate corporate from personal data on mobile devices, is largely responsible for the initial feasibility of COPE. As container technology has matured over the past two years, providing IT departments with more effective and sophisticated mechanisms of carving out separate environments for work and personal use profiles on mobile devices, the attractiveness of COPE has increased proportionally. Containerization is likely to make COPE-based policies more acceptable to enterprise workers with a preference for BYOD by overcoming their reluctance to expose personal information on their devices to the IT department. If users can be assured that their information will be segregated from corporate data and that management activities, such as a data wipe, can be restricted to work-related portions of the device, employees may be more willing to utilize a company-owned device for personal communications and computing activities.

At the same time, containerization is also seen by some IT departments as a means of cutting through the management chaos associated with a BYOD approach, which will only intensify in complexity as a greater diversity of devices enter the organization and mission critical business processes become mobilized. Containerization offerings that deliver common management across multiple mobile operating systems could greatly simplify device and application management for IT specialists, as well as impose a common user experience across a mix of operating systems and devices.

New-found Flexibility

COPE brings new flexibility and adaptability to the never-ending and all-important struggle of IT departments to find the perfect balance of risk mitigation, business enablement and user satisfaction. Though both COBO and BYOD enterprise mobility approaches come in multiple flavors, a COPE-based approach delivers a much broader spectrum of implementation variations, empowering IT to replace the on/off switch that was COBO or BYOD with a shiny new knob that can be turned up or down in small increments. Organizations subject to rigid auditing or compliance requirements, for example, may require a twist to the right to impose stricter rules around network access or data sharing. They may also want to reduce the number of device options offered to end users handling particularly sensitive data. Other businesses may desire a turn of the COPE knob to the left, bringing their enterprise mobility policy closer to a traditional BYOD environment, which is characterized by a diversity of devices and platforms and loosely enforced security.

Additional Benefits

While the ability to enable a single device to be utilized for work and personal use and securing corporate data from leaking out of the enterprise or being compromised through mobile-device-enabled backdoors are the major selling points of a COPE-based mobility management model, CIOs adopting a COPE approach will be in a position to introduce additional security, management and cost-savings advantages not available in a BYOD-based environment, including the following:

- Cut Down Device Chaos: COPE gives IT the ability to limit the diversity of devices and platforms accessing corporate information to a manageable number. By providing end users with a modest but meaningful selection of popular devices, IT departments can achieve the twin objectives of satisfying their user base and significantly reducing device and application management complexity.

△ Back to the Contents

Mobility Litigation Case Files

While management has embraced the anywhere, anytime work environment that mobile broadband and the proliferation of mobile devices has enabled, the rank and file is beginning to push back by filing grievances or seeking compensation through litigation for potential violations of privacy or labor laws. As mobile technology increasingly blurs the line between work and personal life, boundary-defining litigation is likely to increase. Complicating this still-evolving landscape for businesses and organizations, especially multi-nationals, is the fact that laws and cultural morals differ from country to country.

In general, corporations are better protected against legal actions from employees over privacy violations or lost information if the organization has issued and owns the mobile device, making it easier to impose policies that reduce the risk of litigation. Though enterprise mobility case law is relatively new, the early days of BYOD and workforce mobilization have already produced some notable and cautionary legal actions.

The City of Chicago Police Department would have been wise to have applied usage policies to police officers' corporate-issued smartphones. Officers who claimed that messages and voice calls placed to smartphones outside of normal work hours constituted overtime sued the City of Chicago for back pay in 2010 under the Fair Labor Standards Act. While city officials have publically commented that the smartphone activity was part of the officers' normal responsibilities, the lawsuit may have been avoided with a carefully worded user policy or if the police department had configured the smartphones to be unavailable for work-related activities during off hours.

An increase in legal actions related to smartphone usage outside of normal work hours prompted a California law firm specializing in employment law and labor relations to dedicate a blog post to the topic. The May 2, 2013 issue of the California Public Agency Labor & Employment Blog on after-hours smartphone use recommends that companies follow several precautions to avoid potential lawsuits. Included on that list is a recommendation for businesses to reduce risks by monitoring employee access to the network and email.

The potential for labor or privacy lawsuits related to mobile device management, however, is likely even greater outside the United States. Portions of Europe, in particular, are vigilantly protective of workers' rights and the privacy of citizens.

Police officers, this time in Sweden, could end up in legal hot water after mistakenly including a civilian in a chat session about ongoing investigations. The incident, recounted in several published reports from February 2014, involved multiple officers using a popular consumer messaging application to chat about and share images related to ongoing investigations. Though the sensitive information was apparently not distributed beyond the university professor who was inadvertently included in the group chat, leakages of this sort by government agencies could easily result in lawsuits, as well as damaging the reputation of the agency and seriously eroding public trust. A COPE approach to enterprise mobility management provides organizations with several options for reducing or eliminating the risk of sensitive information being leaked through pubic channels.

- Reduce Costs: By buying devices and voice and data service plans in bulk, businesses and organizations can take advantage of volume discounts. This is an especially attractive proposition for organizations that reimburse employees for device purchases and monthly voice and data plans. Corporate control of voice and data plans can also better insulate businesses from bill shock, which results from sometimes-exorbitant charges associated with international roaming.

- Tighten Content Control: A COPE policy, which typically involves the IT department pre-configuring mobile devices with secure containers to separate work and personal data, enables enterprises to keep close tabs on corporate content. In addition to security concerns associated with loose oversight of work-related data and communications, strict tracking of enterprise content is essential for compliance with regulatory requirements, such as eDiscovery or vertical-specific regulations, including the Health Insurance Portability and Accountability Act (HIPAA) or oversight requirements recently imposed on the US financial community in the wake of the 2008 economic crisis.

- Centralize Oversight: A COPE policy provides a streamlined management environment more conducive to the imposition of company-wide policies than BYOD, which often requires separate policies for each business unit. COPE enables standard policy and governance rules for the entire organization, helping to reduce costs related to management complexity.

△ Back to the Contents

- Avoid Litigation: COPE, leveraging the ability of many EMM solutions to partition devices into personal and work-related environments, provides end users with reasonable assurances that their personal data will not be monitored or managed by the corporate IT department or wiped out in the event of a lost or stolen device. In addition to creating more cooperative end users, this COPE attribute could reduce legal actions by employees related to privacy. While the legal waters are largely uncharted in this area, organizations that capture or delete personal information from a mobile device tend to be less exposed to law suits if they own the device, rather than the employee.

COPE: No Panacea

While COPE offers several attractive attributes for efficiently balancing the business enablement, usability and risk management goals of enterprises and organizations of all sizes, its appeal will be less than universal. Some organizations, depending on size and level of security concern, may prefer the openness of BYOD and others may get tripped up by the flexibility of a COPE approach, finding it difficult to fine tune policies to strike a satisfactory balance between the needs of IT, business leaders and workers.

Coming up with the right number and mix of approved devices, for example, could present a challenge. IT administrators who fail to provide users with a sufficient variety of devices are likely to encounter backlash in the form of workers increasingly relying on their own devices. The inability to support specific operating systems may create additional issues. While BlackBerry, iOS and Android dominate the mobile platform spectrum in most businesses, other platforms enjoy pockets of popularity in some markets and geographies. Businesses that do not support these platforms will not be able to attract end users to a COPE enterprise mobility model.

At some level, COPE might not be viewed as a distinctive mobile device policy strategy but simply as a variation of either corporate-liable or BYOD polices. Businesses may discover that providing a middle-ground mobile device strategy, especially one characterized by a large number of variables and permutations, is too complex and expensive to maintain.

Regardless of the attractiveness of a COPE-based enterprise mobility model, a percentage of business users will continue to bring their smartphones and tablets into the workplace. BYOD, in one form or another, is here for the long term. To accommodate an inevitable hybrid COPE-BYOD environment, IT departments need to ensure their EMM solutions are capable of supporting both approaches simultaneously and from a single console.

△ Back to the Contents

Conclusion

The days in which the assignment of a corporate-owned mobile device meant all work and no play are over. Enterprise mobility management has evolved to the point where even highly regulated industries now have the option of allowing workers to use company-issued devices for personal computing and communications activities, such as social media, game playing and other types of digital entertainment. These mobile device and application management advances, along with the rapid acceleration of workforce mobilization and its expected impact on an organization's ability to secure corporate data residing on an increasingly diverse collection of employee-owned devices, is prompting a surge of interest in complements or alternatives to BYOD.

COPE is gaining fresh momentum as a mobile device management model due to its ability to combine the freedom and flexibility of BYOD with the control and oversight of COBO approaches to enterprise mobility. A major component of COPE's appeal is that it offers a potential solution to the conundrum facing enterprises embarking on ambitious workforce mobilization initiatives: how to provide the proper measure of protection of sensitive company information without degrading user experience or impinging upon the ability of business leaders to maximize productivity.

While BYOD has been and will continue to be embraced by enterprises and corporations for its ability to advance worker productivity, it also poses security and management risks that have at times created tension between IT, business leaders and end users. IT leaders in regulated industries, such as government, education, healthcare, financial services and legal, are being inundated by BYOD due to their inability to safely sanction corporate-issued devices for personal use. COPE, with its ability to enable the configuration of company-provided smartphones, tablets and other mobile devices for personal communications and computing activities, offers a pathway to unprecedented alignment of the various constituencies with a stake in advancing the mobilization of the enterprise.

△ Back to the Contents

BlackBerry, a global leader in mobile communications, provides enterprise mobility management and containerization solutions that support a broad spectrum of enterprise mobility policies and deliver an optimal balance of risk management, business productivity and end-user satisfaction across BlackBerry, iOS and Android device platforms.

BlackBerry's ability to support a COPE environment was documented in a 2014 report from Gartner Inc. entitled "Protecting Enterprise Information on Mobile Devices, Using Managed Information Containers." The reported stated that "BlackBerry comes closest to offering a product to support COPE. BlackBerry 10 devices running BlackBerry Enterprise Service 10, Service Pack 2, includes a Personal Space that is separate from the Work Space on the device, and policies can be set as to what the user is allowed to do within the Personal Space. Other container products do not support such a model."

BlackBerry Enterprise Service 10
BES10 is a unified multi-OS device, application and content management platform with integrated security and connectivity enabling you to effectively manage complex enterprise mobility environments. Built for security from the ground up, BES10 makes it simple to manage corporate and BYOD BlackBerry, iOS and Android devices from a single management console. Seamless separation of work and personal content perfectly balances end user and enterprise needs without compromise, while preserving the native user experience.

BlackBerry Balance
BlackBerry® Balance™ technology gives your employees the freedom and privacy they want for their personal use while delivering the security and management you need for business use. It's the best of both worlds, seamlessly built into every BlackBerry® 10 smartphone and managed through BlackBerry Enterprise Service 10. Personal and work apps and information are kept separate, and the user can simply switch from their Personal Space to their Work Space.

Secure Work Space for iOS & Android
Secure Work Space is a containerization, application-wrapping and secure connectivity option that delivers a higher level of control and security to iOS and Android™ devices, all managed through the BES10 administration console. Managed applications are secured and separated from personal apps and data, providing integrated email, calendar and contacts app, an enterprise-level secure browser and secure attachment viewing and editing with Documents To Go™.

BlackBerry®

△ Back to the Contents