COPE, CORE, BYOD? DECIPHERING MOBILITY FOR SMBS

By Melanie Seekins

NOVEMBER 2016 | US$25 | S111116

Channel Partners™

COPE, CORE, BYOD? DECIPHERING MOBILITY FOR SMBS

By Melanie Seekins

NOVEMBER 2016 | US$25 | S111116

Channel Partners™

TABLE OF CONTENTS

Ownership Models 5

COBO 6

COPE. 6

CYOD 7

BYOD 7

Management Tools 8

Device Purchasing Options 8

Big Picture Approach 10

Channel Partners™

ABOUT THE AUTHOR

linkedin.com/in/melanieseekins
@b52junebug

MELANIE SEEKINS went straight from high school in Lander, Wyoming, to the U.S. Navy, where she received training to be an aviation electronics technician on the A-6 Intruder. That training allowed her to excel in the field of telecommunications, wide area networking (WAN) and, ultimately, mobile technologies. During her rise from mobile support to mobile architect, she has worked in many different verticals, developing a broad understanding of the challenges that institutions, organizations and governments face around securing mobile devices and delivering dynamic mobile experiences. Her strategies have enabled multiple businesses to successfully embrace mobile technology and ranked her as a thought leader. An experienced conference speaker and contributor to Information Week and Channel Partners, Seekins is the chair for the Credentialed Mobile Device Security Professional (CMDSP) certification.

COPE, CORE, BYOD? DECIPHERING MOBILITY FOR SMBS

YOUR SMB CUSTOMERS ARE GRAPPLING WITH EMPLOYEES' MOBILITY EXPECTATIONS.

On one side: Workers, especially millennials, are stuck like glue to their smartphones. They expect to work when and where they want and to interact with customers, co-workers and suppliers via mobile. Try issuing them a device that's several years old and rigidly controlled. Today's workforce is not only mobile-savvy and committed to a platform, in most cases, they are inclined to reach for a mobile device first for any task. That's especially so for email.

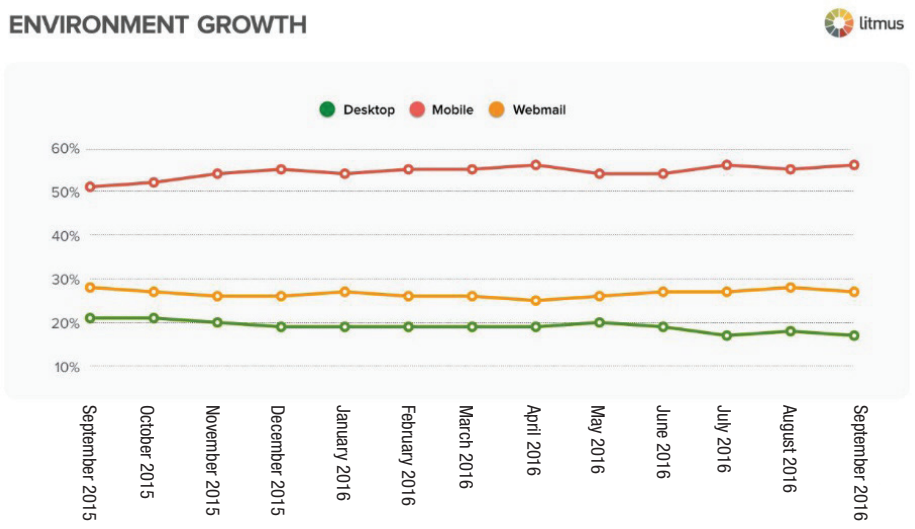
Employers, meanwhile, are struggling with supporting multiple mobile platforms and hundreds of applications, the cost of data plans and devices themselves, data security and backups, what to allow on the network and demonstrating ROI for mobility efforts. They know that smartphones don't get better with age — in its 2016 U.S. Wireless Smartphone Satisfaction Study of 7,500 mobile users, J.D. Power found that people are happier with their devices if they know that they can swap them out annually.

Those who planned to use their phones for less than a year showed the highest satisfaction score — 853 out of 1,000. Those expecting to keep devices for three or more years? Just 817.

Meanwhile, carriers are phasing out subsidies for popular devices. J.D. Power says a shift away from service contracts contributed to growth in the average smartphone price, to $318 from $287 last year. Subsidies are not coming back, leading to new decisions and possibilities.

Most Email Is Opened on Mobile

Based on 1 billion emails sent using Litmus' Email Analytics, mobile opens increased to 56 percent, desktop opens increased to 17 percent and webmail opens decreased to 27 percent between September 2015 and September 2016.



Source: Litmus Blog, September 2016

Your small and midsize customers are foundering, desperate to keep their data safe and employees satisfied without breaking the bank. Partners who can help will increase their stickiness and visibility.

When discussing mobility programs, remember: The goal is always to help the business grow. Educating customers on ways to control spending and meet end-user expectation will be advantageous to both employer and employee.

In this Report, we'll explore common device ownership models — COPE, BYOD, CYOD and COBO — and the differences between management platforms, as well as leasing devices versus purchase given the discontinuation of subsidized mobile phones.

Note that for larger customers, it might make sense to sign on to partner with a telecom expense management (TEM) firm like Asentinel or Tangoe. According to the Telecom Association, the average TEM customer spends about $50,000 per month across fixed and mobile lines. The association suggests that customers need to spend more than $5,000 per month on phone, data and internet and be getting bills from multiple companies for this software to make sense.

Smaller companies need partners' help sorting out options. Here's where to start.

OWNERSHIP MODELS

The first thing customers must decide is whether they will issue devices to employees or let them use their own. There are advantages and disadvantages to each model. We'll look at them from most to least restrictive.

4 Top Recommendations

With BYOD the norm, having at least rudimentary mobile device management (MDM) capabilities is no longer an option. Online services mean that SMBs need not bust the IT budget, nor task their trusted technology partners with lengthy, complex implementation projects.

For businesses without mobile management procedures, we recommend the following:

- Those already using cloud productivity platforms, like Office 365 or Google Apps, should **exploit bundled MDM capabilities**. Deploy to the entire organization and test for a reasonable timeframe. If you find deficiencies, investigate more comprehensive EMM options like Intune (Microsoft) or Android for Work (Google).
- Microsoft shops not yet using Office 365 — whether or not they have SCCM deployed — should **try Intune**. As a SaaS product, it doesn't require new infrastructure and can be incrementally deployed to a subset of users or roles.
- Organizations using an on-premises, third-party systems management suite should **investigate its MDM options**. Most have some functionality, and this may be the easiest route to add mobile control to existing IT management systems.
- Survey the field of **available MDM products targeted to SMBs**. Most providers have free trials and even free service tiers, meaning detailed evaluation and testing costs just consultant or staff time, not software purchase dollars.

COBO

"Corporate Owned, Business Only" is an old concept, but a new term that has been recently floated around in mobility support circles. The COBO device is intended for the employee to conduct official business only; little to no personal use is allowed.

Pros: This ownership model is seen by some organizations, especially large firms, as a way to hold down mobility expenses. It allows for tighter security, smaller data and voice plans, and tightly dictated terms and conditions around use. The employer has the ability to track employees, capture text messages and retain any information placed on the device, as they see fit. This is the corporate version of a secure phone and may be the best choice in regulated industries.

Cons: Employees in this model have a tendency to find workarounds. They often have two devices, one for personal use and one for business, with the latter device utilized only during work hours. Employees may question the amount of information their employer needs and raise privacy complaints. However, recent issues with misuse of mobile devices by employees and security concerns, such as news about HIPAA breaches, could drive some customers into this model.

COPE

The "Corporate Owned, Personally Enabled" device model has been around for years and is enabled by containerization, or sandboxing, technology to separate work and personal data. This model is based on the notion that if a company is going to furnish a device, perhaps allowing the employee to also conduct personal business on it isn't a bad thing.

Pros: With this ownership model, it's more likely that employees will carry their devices all the time. They'll stay more engaged and are more likely to treat the device with care, as it might be the only one they have for work and personal use. It also allows the employer to put caveats around security and the number of different

devices it will support, and to control number portability — important for some types of employees. In the case of a sales professional, for example, being able to transfer a number that customers or vendors are used to calling to a new account rep can be key to keeping those customers.

Cons: In businesses where turnover is high or employees need only basic mobile interactions like email, contacts and calendar, COPE can be overkill. COPE can be very limited as to available device types, capabilities and carriers. If the company doesn't need all the bells and whistles of an Apple iPhone, they may opt for a less expensive Android, possibly causing dissatisfaction with the choice of devices.

CYOD

"Choose Your Own Device" is a fusion of corporate-owned and bring your own. The employer offers a range of devices from which employees may choose, often in a "purchase" model based on an allowance. The key is to present a manageable subset of the wide-open market, thus allowing the help desk staff to support devices appropriately.

Pros: CYOD has been floated as a way to meet the needs of the new workforce, which values choice. The device list is updated as new models come out and, as the employer allows, the employee can regularly switch to a new device. Older models may be retained as loaners.

Cons: If employees in a CYOD model must choose a device blindly, some will be dissatisfied with the outcome. They should be given a chance to interact with the devices on offer before purchasing. This can be at the company help desk, via a partner event or by referral to a retail location — the most common method for small to midsize companies. This way, the employee can be an informed consumer.

BYOD

The "Bring Your Own Device" strategy was once touted as a cost-saving measure. The employer might offer a one-time and/or monthly stipend in exchange for employees using their personal devices for company business. It seemed like a way to ditch the costs of mobile, but before long, problems became clear.

Pros: BYOD allows users to bring in any device and access the company's apps, email and data. This allows high user satisfaction, as people get to use their own devices, and they tend to be more responsible with the hardware, which will cut down on replacements for break/fix issues. They are using a device they're familiar with, which minimizes trivial support calls, and if they want to watch hours of Netflix on a data plan, that's on them.

BYOD Goes Big

Gartner says BYOD is most prevalent in midsize and large organizations — $500 million to $5 billion in revenue, with 2,500 to 5,000 employees. Companies in the United States are twice as likely to allow BYOD as those in Europe.

Cons: BYOD should not be a "bring your own iPhone only" program. This sort of platform limitation can hurt the company more than it helps — a lack of true choice can cause the program to backfire. Not offering a stipend can also be problematic. Employees could choose to not answer a critical call after hours, for example.

In addition, there are security and data management challenges. Well-written policies around the handling of company data must be drawn out and enforceable. The ability to impose certain policies, like location tracking for delivery employees, is limited on a personal device. Not all employees carry a phone tied to a major carrier and thus may experience dead zones. Overages and hitting limits due to purchasing inexpensive data plans may affect the business.

BYOD still requires some sort of enterprise mobile management tool be used with an employee's device to protect company data. The cost for this does not go away based on the device ownership model. BYOD also has been shown to encourage more people to use the program, increasing the cost of back-end support.

MANAGEMENT TOOLS

For cases where a device is used for personal and business tasks, businesses may want to use enterprise mobility management (EMM) tools to set up secure containers, dividing smartphones into two partitions, one for personal use and the other for corporate use. If a device is lost, they can wipe all business data, and they can enforce rules for web browsing and accessing corporate data like email and documents, which may be encrypted inside the container.

There are also mobile application management (MAM) and tools that can control the applications in use on a device, track what data is on the device and perform other functions.

These tools are available in an as-a-service model; we run down more particulars in this Report. And, Microsoft shops should look into InTune or Exchange ActiveSync.

Though rudimentary, ActiveSync can permit administrators and users to set policies for remote full-device wiping, access to company resources and use of complex passwords.

DEVICE PURCHASING OPTIONS

We've seen lots of change in how devices are purchased. In January, AT&T ended subsidized purchases, offering only its AT&T Next installment plans or full retail pricing. T-Mobile and Verizon had already dropped subsidies.

We've seen larger businesses hire a full-time employee just for mobile expense management. For SMBs, deciding among full price cash purchases, device upgrades, leasing programs and payment plans can be extremely confusing. In some cases, these customers may be defaulting to BYOD just so they don't have to sort out leasing terms, caveats for upgrades, carrier subsidies, bulk data plans, insurance and other confusing options.

Take subsidies. They began as a way to entice wireless customers to sign a two-year contract and in return get a phone for a discounted price — or so it seemed. In reality, the full cost to the carrier of the device was accounted for in a higher cost for service plans. This model also locked customers into a two-year agreement.

Get on Policy Patrol

Your customers can enhance the effectiveness of mobile device management tools with a formal, written policy governing how employees may use personally owned devices. Writing up some guidelines costs only a few hours of time; there are a number of free, online guides and templates available, so no one need start from scratch. Some basics:

- **Don't work in a vacuum.** Pull in HR, line-of-business leaders and mobile power users, such as salespeople. Strive for diversity and collaboration rather than making the policy an edict from IT.
- **Be goal-oriented.** What business processes will benefit from mobility? This drives the applications discussion. Email is very different from making a remote connection to the internal network, storing data locally on the device or accessing a SaaS application.
- **Focus on the data.** Valuable and sensitive data should trigger stricter policies. There's no way employees should have lists of customer SSNs, for example, on a mobile device.
- **Formalize the policy.** Define the mobility policy in writing, then have users sign it. Make sure it has teeth — there should be consequences for putting company security at risk. However, the policy should also protect employees by defining when IT may do a remote wipe, any reimbursement for data plans and which personal devices and platforms IT or the help desk will support.

Finally, make it a point to review and update the policy at least yearly. Mobile technology is changing rapidly, and a stale policy is an ineffective policy.

Theoretically, the unsubsidized model that is currently popular with carriers is better for the consumer or small business because monthly phone service plan costs should go down. In many cases, that's not happening, even as the full device cost is pushed to the customer.

Enter leasing programs, which have now become the new big thing from all of the major carriers. AT&T's Next program can sound very appealing. The idea is that an employer or employee pays a set amount each month to purchase a new phone and has the option to easily upgrade to a new model when it's released.

However, there is a caveat that customers may not be aware of. What happens to the business when it needs a new device before the terms for upgrade are met? Say an employee breaks or loses a phone. If another worker is eligible for an upgrade, the customer could in effect use the Next program as a "buddy" device replacement plan for break/fix. This will likely cost more for the customer when a replacement must eventually be paid for in full.

Apple's leasing program also has some lesser-known fees and caveats. For example, each unit purchased under its program must have the two-year Apple Care agreement, which is now rolled into the lease amount. According to Whistle Out, the Upgrade Program is issued through Citizens One Personal Loans; for BYOD, the employee will need to undergo a credit check and have a valid U.S. personal credit card to be eligible. For employer-issued devices, the customer would need to set up an agreement with Apple. A phone in working condition must be turned back in

to upgrade to the next model. And, under the Apple Care program, customers get only two cases of physical damage covered, and even then it's not free. Submitting a phone for repair comes with a $99 service fee, as well as any other applicable taxes.

As most carriers remove subsidies, another option available to small businesses is purchasing the device outright at full cost. While this can be advantageous to the customer — they have a firm grasp on the cost of the device — it can also come with some angst. What happens if an employee loses or breaks a phone?

This is where insurance comes in. Advise customers on fees, the option to select unlocked devices and limits on how many times a device can be replaced in a certain time period. The upside is that the device has been paid for, and the cost for the plan plus insurance can be now be budgeted for.

Speaking of plan costs, owning unlocked devices provides for portability among various carriers. No long-term contract makes it feasible to pick and choose among the major carriers based on employee location and data needs.

BIG PICTURE APPROACH

One of the most critical questions to ask business owners is, "What are your goals for mobile?"

Where are they today, where do they want to be and how long do they have to get there? As you talk to business owners, consider the following approach to ensure that they have accurate information to make an informed decision:

Current cost analysis: The bucket of what the company is currently paying for mobile should include all current voice and data plans, warranties, insurance and device financing or leasing. Also factor in average life span of devices, which will vary based on business type.

Mobile strategy: Partners can help lay the foundation of a solid mobile strategy that will take a small business from ad hoc to a mature plan that will grow with its needs. Address how they are securing their devices and policies that must be in place to protect the organization. Unfortunately, most companies don't grasp the cost of a breach or data loss due to carelessness. In small companies, a lost device that's not password-protected and that has regulated data, like credit card numbers, could be catastrophic. At best, it will take time to win back the trust of customers and suppliers. At worst the financial cost could drive them out of business.

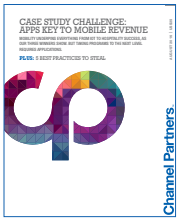
Security topics that need to be addressed include device configuration, anti-malware, anti-theft — the ability to locate and lock a device or erase data remotely, encryption, secure connectivity, application whitelisting and data-loss prevention. Do you need an EMM system, or will Exchange ActiveSync (EAS) suffice?

The strategy should also talk about business capabilities beyond email, contacts and calendars. This can include applications to access documents, secure bids, and execute agreements on the spot. Check out our Report on apps that took mobility strategies, and partner revenues, to the next level.

The right device for the job: Not every employee needs the most powerful iPhone, much as that may pain them. For customers in the service industry, perhaps a ruggedized Android device would serve better.

The right plan for the business: The service plan is a key component of an ownership model. After the cost analysis, you may find that a pooled plan with a set amount of sharable data and unlimited voice and text saves the company money over paying for several plans with different levels of data and calling. The goal is to get mobile plan costs to a fixed amount that allows a small customer visibility into what's often a large investment.

Related Reports



Case Study Challenge: Apps Key to Mobile Revenue

Mobility has changed the way business is done. And as the three winners of our Q3 Case Study Challenge demonstrate, apps are key to taking mobility strategies to the next level.

Mobile Security: 9 Discussion Points to Make the Sale

Yes, it can be a struggle to mitigate the very real risks of an on-the-go workforce without negating the productivity benefits. But the worst thing a customer can do is ignore mobile security. In this Report, we give you some talking points to start the discussion.

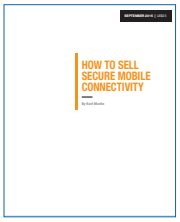
Success Stories: Mobility That Exceeds Expectations

We hear a lot about "overpromising and underdelivering." Our three mobility Success Story winners bucked that trend. The result? Delighted customers.

Case Study Challenge: Mobile Key to Vertical Success

Two of our three profiled solutions serve the health care vertical — a natural for mobility. The third? Well, there's pizza. This Report spotlights Case Study Challenge submissions from Fusion PPT, Broadview Networks and Unified Office.

How to Sell Secure Mobile Connectivity



Of the nearly 1 billion mobile business connections that will be in place by 2017 according to IDC, few stick to managed, relatively secure wireless carrier networks. And at one time or another, most use public Wi-Fi hotspots, which are notoriously easy prey for hackers. It's unlikely employers can keep employees from using hotspots, so channel partners must take steps to educate and protect business customers. This Report takes a look at hotspot hacking and how businesses with mobile users can protect themselves.