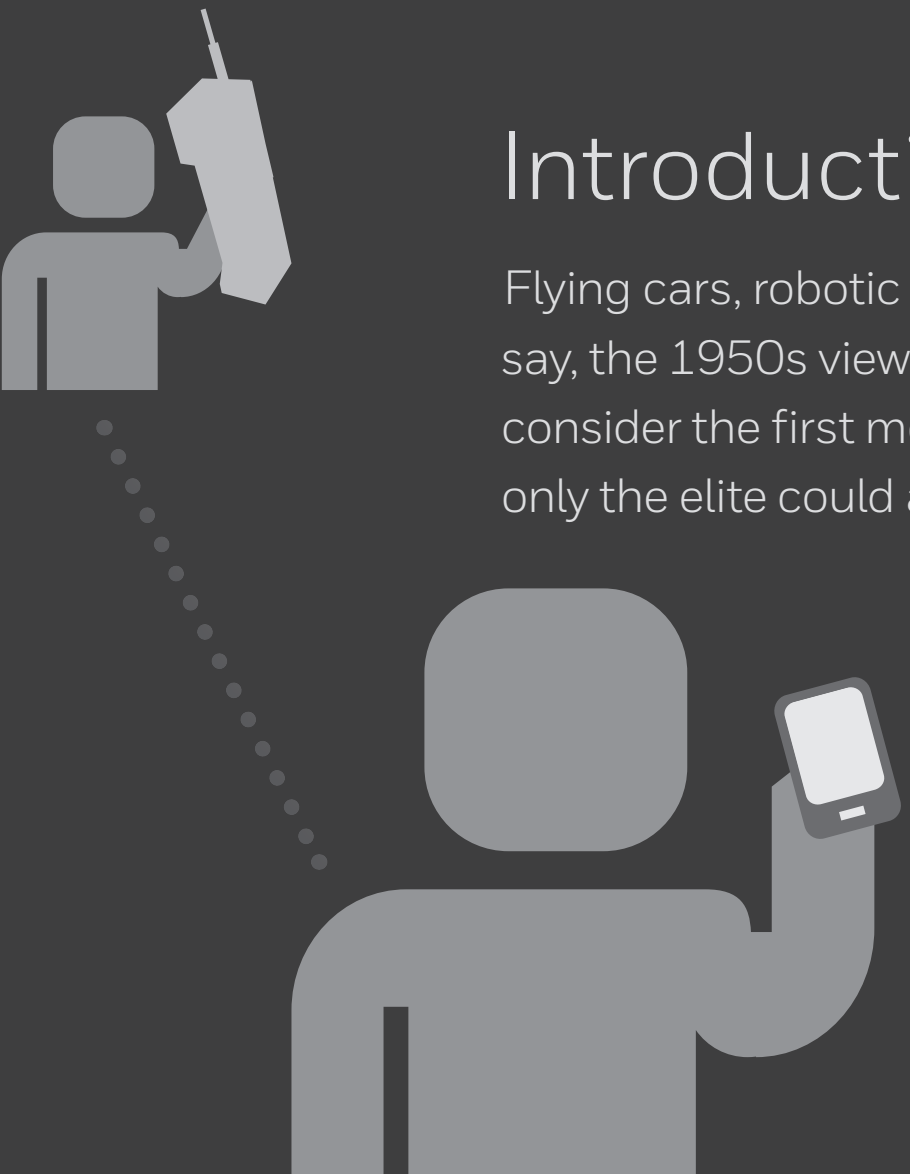
Honeywell

THE ESSENTIAL GUIDE TO ENTERPRISE MOBILITY



Introduction

Flying cars, robotic housemaids, farming on the moon? Needless to say, the 1950s view of the future hasn't fully materialized. But when you consider the first mobile phones – those enormous heavy bricks that only the elite could afford – it's amazing to see how far we've come.

Some of the mobile capabilities that we now take for granted weren't even a possibility a few decades ago. Yet scientists and engineers continue to push the envelope, bringing us an ever-growing number of mobile device types, enterprise apps and unique ways to straddle the corporate and personal worlds.

There has already been an upsurge in innovative advancements such as wearables, with sci-fi-inspired gadgets available for purchase at all kinds of retailers. The trend toward cloud services will continue, but with an emphasis on mobile devices and apps for easy access to files from anywhere. Malware on mobile devices is growing, the mobile device management (MDM) market is consolidating and we're seeing an increased MDM focus on helping organizations grow the return on their mobility investments.

So how do you ensure that your mobile infrastructure is ready for whatever comes next? If you put in the strategic thinking and hard work now, you can rest easier knowing that your mobile environment is doing everything possible to foster employee productivity, increase responsiveness to customers and conserve costs. Read on to learn more about everything from strategic planning for the mobile landscape to supporting the revolving door of devices, apps and content. See how the separate components of your mobile infrastructure can work together to help you achieve a holistic environment that benefits you, your employees and your customers.

Nobody really knows which notions of the future will come to pass. But savvy IT professionals will take advantage of today's mobile possibilities while preparing their organizations for whatever comes flying down the road tomorrow. Be ready.

Enterprise Mobility Planning

WHY A MOBILITY STRATEGY MATTERS

Mobility is all about responsiveness, productivity and efficiency. But jumping into the sea of mobility without strapping on a life jacket won't help your company swim faster... or even stay afloat.

LOOK BEFORE YOU LEAP: WHY A MOBILITY STRATEGY MATTERS

Mobility is all about responsiveness, productivity and efficiency. But jumping into the sea of mobility without strapping on a life jacket won't help your company swim faster... or even stay afloat. You need to define your enterprise mobility strategy, which means stepping back and taking the time necessary to get it right, both for today and for tomorrow. After all, without a strategy, you may be not only wasting money and duplicating effort but also putting your corporate data, business customers and long-term business goals at risk.

ALIGNMENT ADJUSTMENT

If you don't consider your overall business goals as you develop a mobility strategy, you risk investing in mobile technology for mobility's sake alone. Your mobile environment doesn't exist in a vacuum. Employees who use mobile devices also need to use line-of-business apps, data stored on the corporate network and numerous other tools to do their work. By aligning your mobility strategy with the rest of your business, you'll create happier employees and customers.

Also consider the flip side. If you're making other kinds of changes to your IT environment, remember to take mobility into account.

THINKING AHEAD

Smart decisions make it easier to adapt over time while keeping a lid on costs. Skyrocketing mobility costs is a common fear for CIOs, but careful planning will help keep your mobility spend safely earthbound.

It's tempting to race in and grab the latest and greatest devices, but taking the time to form a comprehensive strategy will result in long-term benefits. That planning may include some up-front costs – such as consulting fees if you choose to work with an outside mobility strategist – but a small investment now will yield large dividends later in the form of heightened employee productivity, streamlined management and the ability to take advantage of economies of scale.

MOBILE ACCESS = ENGAGEMENT = REVENUE

"The mobile Internet ecosystem is fragmented, under-serving the needs of people, businesses and brands."

– **MOBILE WORLD CONGRESS**, 2015

MAP YOUR PATH: HOW TO ESTABLISH THE RIGHT STRATEGY

Gone are the days when mobility involved simply choosing a standardized device. Today, you have to think about not just devices but also apps, data, storage, management (of devices, apps, content and telecom expenses) and support. Each plays an integral part of a successful mobility strategy.

TAKE STOCK

Before you start to make purchasing decisions, you need a true understanding of your current state, including your application architecture and your business requirements. Without knowing what you have, you won't be able to make sound financial decisions about what you need. Analyze your infrastructure and processes and consider how you'd like to translate them into the mobile world. Think about your existing technology investments and those that could apply to your mobile strategy.

Of course, it's also important to evaluate your competition and what's going on in your industry in terms of enterprise mobility. Is a cool app from one of your competitors leeching away your market share? How can you capture the interest of their customers and make sure to keep your own? Knowing what other companies are doing – seeing what works and, perhaps more important, what doesn't work – can help shape your own mobility goals.

GRASSROOTS SUPPORT

When it comes to establishing a mobility strategy, you can't go it alone. Soliciting buy-in from key stakeholders results in a larger pool of ideas, greater adoption and less frustration later. Get input from all angles by forming a cross-functional team to help determine what makes your business tick. Working together will also give you a stronger sense of the specific issues and opportunities that your mobile strategy should address.

Have your team identify all the ways that different roles in your workforce currently use mobility, and explore other areas that are ripe for enhancement. Together, you'll get a complete view of how many ways mobility could play a positive role in your company's future.

DIVISIVE DEVICES

It's a given that stakeholders will have strong opinions about which devices are right for them. And with new devices flooding the market every year, it can be a balancing act to stay current without breaking the bank. One of the most critical decisions that many companies have to make is which mobile platform to choose. Establishing a standardized platform helps other elements – such as apps and support – fall into place with minimal hassle. The bring-your-own-device (BYOD) model is growing in popularity, and it can spare you some difficult decisions, but it also presents a whole series of considerations: How expensive will it be to support a BYOD program? How does our BYOD program affect our ability to provide custom apps? Should we use stipends to help users acquire their own devices and plans? Are we opening ourselves up to potential legal ramifications? Do we need additional security software to help mitigate risks?

DOWNLOAD HONEYWELL'S BYOD POLICY TEMPLATE FOR:

- A comprehensive list of key elements to include in your policy
- Tips on stronger security for your mobile enterprise
- Guidance on how a BYOD policy can save you time and money
- Ways to realize the full potential of your BYOD environment

If you opt for a corporate, non-BYOD approach, you'll need to determine the right platform and recognize which devices straddle the fine line between cost-effective use of company resources and user acceptability. After all, if employees don't like the devices you choose, they won't use them, which would be a waste of time, energy and budget. Putting into employees' hands devices that tie into your existing infrastructure, run necessary apps and heighten productivity will have a major influence on adoption.

"2015 will be the year of the mobile app. With one in five tablet purchases being for enterprise use alone, the numbers back us up... IT organizations will dedicate at least 25 percent of their software budgets to mobile application development, deployment and management by 2017."

– **ORRIN BROBERG**, App Data Room

AN APP A DAY

More and more, software companies are investing in mobile versions of their enterprise apps, but that doesn't necessarily mean those apps are right for you. Having native compatibility between desktop and mobile devices seems logical, but you have to make sure that those mobile apps meet your company's needs. It may be that other off-the-shelf apps make more sense, or you may want to develop your own.

Would it work best to use the cloud to serve up your apps? Do you plan to virtualize them? Do you want to provide for a range of platforms? Knowing the answers to these questions will help you formulate a mobile app strategy that will serve you well both now and in the future.

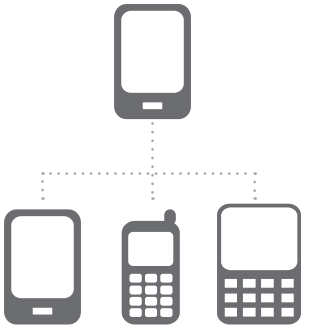
PROTECT THE CROWN JEWELS

If desktop security breaches make you need to breathe into a bag, imagine the risks involved in putting corporate data on devices that employees take on business trips, out to lunch and even on vacations. Safeguarding those devices – and the data that's stored on them – should be among your highest priorities.

Here's the good news: Devices and mobile software apps now include more security features than ever before, so it's easier to lock down devices, wipe them if they get lost or stolen, and establish appropriate checkpoints to secure access to corporate data. Mobility management solutions (including mobile device management, mobile application management and mobile content management tools) offer additional layers of security, so you can tailor settings and access to your users, devices and apps based on the sensitivity of your data. Plus, the industry is adapting with comprehensive security solutions like Samsung Knox, recently made available to all users on any Samsung device.

A secure BYOD environment must achieve the following goals:

- Space isolation
- Corporate data protection
- Security policy enforcement
- True space isolation
- Nonintrusiveness
- Low resource consumption



DID YOU KNOW?

According to Gartner, BYOD is growing fast – by 2016, 38 percent of companies will stop providing their employees with devices. By 2017, the same survey predicts, that figure will rise to 50 percent.

IT'S POLICY

"Policy" can be a dirty word in the IT realm, but putting the right policies in place can be critical to successful enterprise mobility. They can make a difference in ease of use, cost, IT control, security... the list goes on. Make sure you're clear on your policy goals, because it's easy to lose sight of the fact that you are trying to protect content, and find yourself concentrating on cost savings instead.

- Decide on relevant acceptable-use policies to determine which apps are approved and which are blacklisted.
- Make certain that sensitive data is properly encrypted and available only to those who should have it.
- Do everything you can to ensure that your devices don't provide an open door to your corporate data.

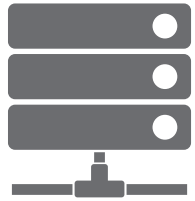
The more you lock down your devices, apps and content, the less freedom your employees have. While slowing down employees too much can have a negative effect on their productivity, making them think before barreling ahead in an insecure direction can be worth a small hassle. But try to avoid presenting policy hurdles that are too big, because they tend to result in users who work around – rather than within – your setup. Be as transparent about your policies as possible.

Employees need to know what's fair game and what's off-limits, and they also should be aware of the company's rights and responsibilities (and their own) if a device is compromised.

BE SUPPORTIVE

Adding a mobile infrastructure – especially if you have a BYOD program, with its myriad device types and platforms – can overload a helpdesk, and IT staff may be ill-equipped to deal with mobility issues. Be aware of your support structure and bandwidth constraints, and make sure that you have enough of the right kind of expertise sitting at your helpdesk. And, because the whole idea of mobility is to be able to work from anywhere at any time, you'll truly need 24x7 support.

You may decide that training your current helpdesk staff makes sense, and you may even need to add a few heads to the group. (Remember, it's not uncommon for employees to have more than one mobile device, so the uptick in support demands may be even steeper than you anticipate.) Many companies decide that their mobile environments require a dedicated leader, board or team beyond the helpdesk, and some opt to turn over support entirely, relying instead on expert outsourced partners for more consistent costs and service.



DID YOU KNOW?

BYOD policies create an insecure environment, as the corporate network is extended and becomes harder to protect from attacks. In this scenario, corporate information can be leaked, personal and corporate spaces are not separated, it is difficult to enforce security policies on the devices, and employees are worried about their privacy.

KEEP TABS

Once you've done the heavy lifting and have your mobile environment up and running smoothly, make sure it stays that way. Lots of organizations overlook the importance of monitoring; including monitoring services in your initial strategy ensures that your mobile environment will keep working for you. Make sure you properly handle posture monitoring so that you know how many of your devices are quarantined, part of a BYOD program and so on.

Just as the car that was state of the art a decade ago no longer turns heads, advancements in mobile technology make today's must-have features old news pretty quickly. If you continuously monitor your device and app usage, you'll have insights into which investments are paying off and which are no longer necessary. At the same time, by keeping an eye out for new technologies, you can take advantage of efficiencies across your mobile enterprise. To really get the most out of your mobile environment, also monitor security and costs – many companies use telecom expense management (TEM) software to track and manage wireless assets.

DID YOU KNOW?

Given that mobility is a key enabler of digital businesses, it should come as no surprise that mobility is a strong area of focus for all types of companies. Indeed, 4 in 10 companies indicated that they have aggressively pursued and invested in mobile technologies across their business, and that they consider mobility to be a key part of their business strategy.

TRACK MOBILITY TRENDS: WHAT TO WATCH FOR AS YOU MOVE FORWARD

Speaking of trends and taking advantage of them, here are a few things to keep in mind as you embark on your mobility journey:

Relevant apps. It used to be the devices that got all the attention, but apps now play a greater role in strategic decision making.

Forrester notes that 35 percent of large enterprises will use mobile application development platforms to develop and deploy mobile apps across their organizations in 2015. By 2017, 100 percent of line-of-business (LOB) apps in internally facing roles will be built for mobile-first consumption.

Keeping up with devices. For plenty of employees, having a smartphone isn't enough. They also want the option to use a laptop, a tablet or even a multimedia player. As other devices and related technologies emerge, such as sensor fusion and the Apple Watch®, companies need to stay aware of the changing landscape.

The move to HTML5. Although native apps usually provide a greater experience than web apps, web apps using HTML5 are closing the gap and have the benefit of running on multiple mobile platforms. Because some apps are best suited for native environments and others work better as web apps, many companies are considering hybrid apps as a compromise that meets the needs of both developers and users.

Cloud and virtualization. A growing number of companies are turning to cloud-based mobile apps and virtualized apps to store data more securely. The cloud provides added incentives, including accessibility to data from multiple devices, low costs and increased performance speed.

DID YOU KNOW?

In a recent Accenture study, 62 percent of respondents said that adopting cloud technology is an important priority. The same survey found that nearly half want to improve their apps, with a focus on reliability and user satisfaction.

BYO... According to a survey by analyst house Ovum, 74 percent of employees use personal devices, apps and other technology at work, essentially bringing them in behind the IT department's back. Faced with this reality, many companies are embracing BYOD as more than just a passing fad, and they're even going beyond it to include other personal resources.

Social media. Twitter and its counterparts aren't just for teenagers anymore. Companies use social media to improve collaboration among employees, build a cohesive brand and celebrate business wins.

Business intelligence (BI). Using mobile devices for visualization and analysis is becoming increasingly common as software developers bring big data to small screens, using the cloud to store the information required to deliver BI insights.

With strategic planning and a forward-looking attitude, you'll be able to properly navigate the seas of mobility.

SOURCES

1. Mobile Apps Increase Enterprise Performance and Productivity Advantages, Top Three Mobile App Strategies Gain Momentum
2. The Rise of Mobile
3. Ovum: BYOD Is Here to Stay
4. 15 Tech Trends to Emerge by 2014
5. Combining ISMS with Strategic Management: The Case of BYOD
6. ZDNet, Adopting BYOD
7. University of Nebraska, Remote Mobile Screen: An Approach for Secure BYOD Environments
8. App Data Room, Honeywell Facts
9. Accenture Digital, Growing the Digital Business, Accenture Mobility Research
10. Accenture, Mobility: Fueling the Digital Surge

FOLLOW US:

Mobile Application Development

WHY APP DECISIONS MAY BE THE MOST IMPORTANT ONES YOU MAKE

Today's employees want more – and they need more – if they're going to stay productive from anywhere, which tends to be the primary goal of having mobile devices in the first place.

APPLICATION CONSTERNATION: WHY APP DECISIONS MAY BE THE MOST IMPORTANT ONES YOU MAKE

Remember the good old days, say, five or six years ago? You could give employees smartphones to use for email and web surfing, and voilà! You had happy employees. Well, email and web connectivity are now just the tip of the iceberg. Employees today want more – and they need more – if they're going to stay productive from anywhere, which is usually the primary goal of having mobile devices in the first place. From corporate line-of-business applications to on-the-go sales tools, employees expect comprehensive corporate information at their fingertips. For them, a mobile device should offer comparable functionality to their desktop environments.

Of course, mobility isn't just for the benefit of employees – there are business benefits, too. Mobile devices should help you realize the mobility trifecta: enhanced employee productivity, lower total costs and increased profitability.

ALL THE ANGLES

A scattershot approach to mobile apps will give you a mobile environment that's full of holes. Companies should provide their employees with mobile apps that are relevant to them, but a lot of thought needs to go into a larger app strategy for the company. Before you invest in off-the-shelf or custom-built apps, make sure you know what your employees' needs truly are and understand the company's overall mobile strategy. You also need to consider the technology that supports your mobile environment, including device types, management tools and network and security requirements.

BIRD'S-EYE VIEW

Next challenge? Delivering the mobile capabilities and information that employees need, while keeping costs manageable and safeguarding your content. First, determine the types of apps that employees are likely to need.

Of course, there's an endless number of specific apps that you could incorporate into your mobile environment, but consider these 10 high-level categories and decide whether they apply to your mobile employees:

1. Business intelligence (BI) reporting
2. Customer relationship management (CRM)
3. Custom internal workforce
4. Mobile-optimized intranet access
5. Field services (dispatch, work orders)
6. Custom sales tools
7. Human resource management
8. Travel and expenses
9. Enterprise resource planning (ERP)
10. Email/calendar/contacts

BEST OF BOTH WORLDS

For employees, having a range of productivity apps on their devices gives them a welcome efficiency boost. Life is even better when their personal apps can peacefully coexist on those same devices. The rise of bring-your-own-device (BYOD) programs makes app management more difficult for IT departments, which need to keep everything secure and maintain the ability to wipe devices without affecting personal information.

The intermingling of business and personal information on one device changes how people operate. Social media apps, for example, often bridge the business/personal gulf, with employees using those sites to manage both their personal brand and that of the business.

IF THE SHOE FITS

In a perfect world, you would address all your app needs with an affordable, off-the- shelf product. And it can happen! More and more, software companies are making sure that their products smoothly extend to the web. But sometimes a standard app just won't do and you need custom functionality to really hit the mark.

Custom apps can be expensive, not just in terms of initial development but also because of ongoing management. Aim to strike a balance between the degree of customization that you truly require and the costs involved.

Fifty-six percent of mobile leaders surveyed say it takes from seven months to more than a year to build a single app. Eighteen percent say they spend $500,000–$1,000,000 per app, with an average of $270,000 per app.

A survey by Clutch of 12 "leading mobile application development companies" found that "the median cost range is between $37,913 and $171,450, but could climb up to $500,000 or higher." The report, released in January 2015, includes detailed breakdowns of cost drivers both as estimates and as descriptive quotes from development company representatives.

DID YOU KNOW?

Apps built by the largest app companies are likely to cost between $500,000 and $1 million to make.

Apps built by agencies, such as Savvy Apps, cost between $150,000 and $450,000.

Apps built by smaller shops, possibly with only two to three staff, usually cost from $50,000 to $100,000.

HOW TO CREATE MOBILE APPS THAT YOUR EMPLOYEES WILL ACTUALLY USE

Now that you've figured out your app needs, identify which of your company's existing desktop applications can be extended to a mobile environment. By offering that desktop functionality on mobile devices, you'll be giving your employees apps that are familiar, comfortable and intuitive. You'll also likely have an easier time connecting your back-end systems to your mobile environment than if you were to bring in completely separate mobile apps.

BRIDGE THE GAP

If you have some areas where you can use existing resources but you're still missing functionality, explore the mobile app market and see what's out there that fits the bill… or that might fit the bill if you made a few tweaks. Customizing off-the-shelf apps will be less expensive than developing your own from scratch because most of the heavy lifting will already be done for you.

According to ABI Research, the global app market has surpassed $30 billion.

An earlier study by Yankee Group placed the value of the North American mobile apps and cloud segment at $85 billion. Its staggering 41 percent growth forecasted by 2017 appears to be on target.

IF YOU BUILD IT…

So you've exhausted all your options for off-the-shelf mobile apps and decided to go it alone. If you're going to embark on a custom mobile app journey, first consider your audience and goals. Find out more about how your users work, and stay in touch with them throughout the whole process to make sure that your app is usable, intuitive and appealing.

GOING NATIVE? WORKING THE WEB? (OR BOTH?)

The next decision is a biggie: whether to develop native apps, web apps or hybrid apps. That decision may not apply to your whole mobile environment – you may decide that some aspects of the business make more sense with web apps while others would benefit most from native ones. Make sure that it's your business requirements that determine your development path(s).

Let's review some of the pros and cons of different types of apps:

Native apps make use of the programming languages, plug-ins and application programming interfaces (APIs) related to a specific mobile device, such as Apple or Android™ smartphones. They have the advantage of making the most

DID YOU KNOW?

The basic consumer app is a mere trifle when compared with true enterprise apps in terms of complexity and costs. When developing a mission-critical enterprise app, it's important to look at every element, including throughput of data, transaction storming, system failover plans, master data protection, integrity and any need for the app to run offline and reconnect when a connection is available. If you don't have experience with this level of custom app development, consider working with a partner to make sure that your app covers all your bases and can also evolve and scale.

of a device's features and full functionality (such as location services), but you'll have to write multiple versions of each app if you have a heterogeneous (or BYOD) mobile environment.

Web apps are a "write-once, run-anywhere" option because they use a web-based client to deliver the corporate or cloud-based data that mobile users need. Programmers can use HTML, which is generally familiar to them, making the development process an efficient one. However, web apps tend not to be as sophisticated as native apps because web apps are one-size-fits-all by definition.

Hybrid apps are a new app type that uses web-based code for the bulk of the app but adds native code and plug-ins to make use of proprietary device functionality. Hybrid apps are growing in popularity because of the momentum of HTML5, which delivers strong interactive and animation capabilities and has the advantage of running on multiple platforms.

Whether you choose native, web or hybrid apps, consider hosting your server-side logic in the cloud. That will give you the chance to create more robust apps that can quickly unlock data from backend systems. Look across your mobile environment and bring together common functions such as authentication, compliance and security to reduce overall development costs through reuse.

THE PLATFORM'S THE THING

Perhaps the nature of your business calls for native apps for some or all of your mobile functionality. You'll need to consider which platform(s) to build on, based on your devices and internal expertise. You may decide to rely on a development partner to do a significant share of the work.

Many mobile app developers choose to work in a cross-platform framework – there are lots of choices out there – that makes it possible to quickly build code and use your initial code base to extend to other platforms. These frameworks are particularly helpful if you have multiple operating systems at play in your mobile environment, making it easier to achieve the write-once, run-anywhere development goal while still creating complex native apps for your employees.

DELIVERING, SUPPORTING AND SECURING MOBILE APPS

You've done it – you have a suite of mobile apps ready for your workforce. But managing those mobile apps has never been more complicated. Take a holistic management approach and determine how you want to deploy apps, where you want them to run, whether they need to be isolated from other processes (or whether their data does), where data from the apps should be stored, etc.

KEEPING ORDER

Employees appreciate having a wealth of apps at their disposal. Ensuring that employees have the right access will help reduce headaches for your IT staff and foster the overall productivity gains that you're looking for. Many companies use mobile application management (MAM) solutions to help distribute and manage their enterprise apps. These solutions include everything necessary to keep apps flowing, from user authentication and access control to push services, event management and reporting.

One of the biggest features of today's MAM solutions is the enterprise app store. Imagine having a branded version of the consumer app stores tailored for your employees and company. Putting an enterprise app store in place not only makes it easy for your employees to get the apps they need, it also deters them from downloading potentially dangerous (and unsanctioned) apps to their devices.

Today, it's estimated that 25 percent of enterprises will have their own app store by 2017. And these enterprise app stores aren't just for custom mobile apps – the good ones will also include third-party apps and links to public app stores and enterprise content. That still leaves plenty of room for growth that would benefit from expert help.

CROSSING THE DIVIDE

Companies also use MAM solutions to make sure that their apps are set up correctly and securely through proper provisioning. These solutions are particularly helpful for keeping corporate and personal data distinct, enabling a "dual-persona" environment on a single device. For instance, security policies can be applied to individual corporate apps, while Temple Run, Facebook, StockGuru and other personal apps can be left unmanaged.

But MAM solutions have progressed beyond basic security. It's now possible for all the corporate apps on an employee's device to communicate with each other and to be managed with a single system. You can implement policies for remote wiping, virtual private networks (VPNs) and corporate app interaction with unmanaged apps. It's even possible

DID YOU KNOW?

When it comes to mobile apps, a growing number of organizations are leaning toward building instead of buying apps, especially when different parts of the enterprise need different custom capabilities.

For instance, according to a CompTIA study, 70 percent of companies have made some level of investment in building mobility solutions.

to keep corporate data from leaking into personal apps and to place limits so that only corporate apps, for example, can open documents and links.

PARTING IS SUCH SWEET SORROW

You never want to think about it, but sometimes valued employees leave the company. It's important to know who owns the data on an employee's device before that employee departs, especially in a BYOD environment. If you have segregated corporate and personal data, it's easier to determine who owns what. Keep careful track of where all data can be stored so that you can better protect that data. For example, if an employee backed up data to iCloud and is now leaving the company, simply wiping the device won't do the trick.

Regardless, you need an effective process for removing corporate email account(s), calendar(s) and contact information from an employee's device without disturbing any personal information. A good MAM solution will ensure that you're in control of your apps and where they live.

By thinking ahead on the app front, you're better positioned to achieve that mobility trifecta of enhanced employee productivity, lower total costs and increased profitability.

SOURCES

1. Figuring the Costs of Custom Mobile Business App Development
2. Enterprise Mobile Apps: Old School, New Rules
3. The Enterprise App Store – Just Another Buzzword or Powerful Business Enabler?
4. App Data Room, Honeywell Facts
5. ABI Research, 44 Billion Mobile App Downloads by 2016
6. Yankee Group, Mobile Metrics to Forecast the Future of the New Mobile Economy
7. Gartner, 25 Percent of Enterprises Will Have an Enterprise App Store
8. Apperian, Enterprise App Stores: Building and Populating the Apps that Matter Most

FOLLOW US:

Enterprise Mobility Deployment

HOW TO GET DEPLOYMENT RIGHT

Configuring and securing a device for corporate use requires know-how and time that most employees just don't have. Getting it right (the first time!) helps keep support costs low and employee morale high.

STRATEGIC READINESS: HOW TO GET DEPLOYMENT RIGHT

There's more to deployment than simply handing out mobile devices to your employees. A lot of thought – not to mention time and effort – needs to go into ensuring that new mobile devices are usable. Configuring and securing a device for corporate use, loading it with relevant apps and managing updates requires know-how and time that most employees just don't have. Getting it right (the first time!) helps keep support costs low and employee morale high.

DON'T BOIL THE OCEAN

Sure, there are occasions when you absolutely have to get a device into a user's hands immediately, but that's certainly not the ideal situation.

Pressure from both management and employees to rush the deployment process shouldn't keep you from maintaining a phased approach. Even those who yell the loudest would be better off waiting until you have a deployment framework in place and can roll out devices in a strategic way.

Measured rollouts give you a better sense of adoption, use and the impact of increased mobility on your helpdesk. By keeping your focus on where you can increase productivity and gain business advantage, you'll be able to stay ahead of the game and foster smart spending.

THE DEVIL IS IN THE DETAILS

After you've determined the best strategy for your deployment, you'll need to be sure that your devices are truly ready to go. Correctly configuring and securing devices is key to a successful deployment. Your employees should be able to unpack their devices and use them, right out of the box.

Here are a few things to keep in mind:

Settings. Most companies choose to use a mobile device management (MDM) solution to handle the lion's share of configuration and management. These solutions are great, but not every setting can be enforced through them. In some cases, you may need to write customized scripts to standardize settings across devices.

Apps. Deployment doesn't just apply to devices. As part of your deployment, you may need to look into code signing (validating the source and authenticity of the software code), app wrapping (applying a management layer to your mobile

app), and containerization (encrypting enterprise apps and separating them from personal ones).

Unique needs. Not all devices fit all user needs. You may have some departments, job roles or individuals who need something different. In special cases, it may be necessary to personalize devices and apps for a target end user.

Documentation. Like any part of your technology infrastructure, it's important to document how you're handling all aspects of your mobile environment. Institutionalizing the knowledge that you've gained throughout the process will ensure that nobody has to reinvent the wheel when changes need to be made.

ACCESSORIZE

Remember, your employees need more than just the devices themselves. Think ahead about the right cables, adaptors and any other power accessories that employees may need for their devices. Beyond power, users may also need screen protectors, cases, vehicle mounts, etc. Making these decisions now will help you take advantage of economies of scale when purchasing.

STICK TOGETHER

Mobile devices can be major productivity boosters, as long as they work properly. Because downtime on a mobile device can be even more concerning than downtime on an office computer, many companies empower their employees to take action. During deployment, IT staff apply stickers on corporate mobile devices so that employees will know how to get support. Immediately knowing what to do in case of a device failure or issue can make a real difference, especially for field and sales employees in situations when time is of the essence.

KEY DEPLOYMENT CONSIDERATIONS

Do you have support from all business areas – including finance, business users, IT and project managers – and are they prepared for deployment?

Does your company have the resources and shipping expertise for a massive deployment?

Will this project take resources (especially IT) away from typical roles and responsibilities? If so, how will you address those concerns?

Does your company have the technical knowledge to get the devices activated and to troubleshoot them?

Do you have a plan in place for handling dead-on-arrival devices?

CIRCUMSTANTIAL EVIDENCE: FOR WHEN MEASURED ROLLOUTS AREN'T AN OPTION

A measured, controlled rollout of corporate devices sounds pretty good, doesn't it? Unfortunately, today's rapidly changing business landscape can make that idyllic scenario impossible. Whether it's a deployment fire drill or a bring-your-own-device (BYOD) quagmire, you'll likely have to think beyond the plan when it comes to mobile deployments.

THE NEED FOR SPEED

You do what you can to plan ahead, strategize and have a mobile deployment framework in place to cover any eventuality. Inevitably, plans change, executives make snap decisions, teams need devices in a hurry and you're put in a tough position: meet the short-term needs of the business and cause yourself a lot of grief, or deny the request and stick to your plan. Maybe there's a meeting coming up soon where thousands of field salespeople will be in one place, and the sales manager wants to roll out devices all at once. Maybe there's a new initiative that your HR department needs to support that requires immediate use of tablets. Sometimes the customers – in this case, your business users – have to be right, and you're in a position where you need to accommodate.

THE PERILS OF RAPID DEPLOYMENT

If you're pressured into a rapid deployment scenario, be as prepared as possible. To start, make sure that you have access to the equipment you need. Be warned: Most new mobile device models aren't available in larger quantities. For example, it's tough to get your hands on thousands of the latest iPhone® devices until they have been on the market for a while. The same may be true for accessories and other items that are crucial to your deployment.

Working within a tight timeline may also require you to bump up your staffing levels, and you may want to consider running multiple shifts to handle the additional volume. Also consider the physical space you'll be working in: Do you have enough room to sit down and configure many devices at once? Do you have enough outlets to plug in large quantities of devices at the same time?

Put some quality control procedures in place so that you know your team is properly handling configuration and its various steps.

In many scenarios, it may be possible to use barcode labels to automate input and reduce the chance of human error.

SELF-SERVICE?

Perhaps your company has started down the BYOD path, which means that you have a more limited role in deployment. Yet you may not be completely absolved from deployment-related issues; many companies that have BYOD programs still assist their employees in the purchasing process to make sure that only relevant devices are joined to the corporate network. It's not uncommon for companies to identify a set of devices that qualify as part of their BYOD programs. While you can't obligate employees to invest in one specific device, you can encourage them to buy preferred devices by offering some type of incentive or reimbursement.

Plenty of device manufacturers and resellers have programs that help companies implement their BYOD initiatives. These programs can include tailored e-commerce websites that offer BYOD-qualified devices, campaign materials, custom pricing for your employees, discounts and promotions, and a range of payment options.

Many companies that have BYOD programs still assist their employees in the purchasing process to make sure that only relevant devices are joined to the corporate network.

THE SPECIAL SAUCE: HOW TO MAKE MOBILITY A LONG-TERM SUCCESS

Technology projects have multiple aspects that go into making them viable. Mobile deployments are no different. If you want to achieve the productivity and return-on-investment (ROI) gains that mobility can offer, you'll have to consider the entire deployment process – and beyond – before embarking on a rollout.

BUY NOW AND SAVE!

Getting the right purchasing plan in place might be the first step in a successful mobile deployment. There are lots of options for procuring devices, from working with resellers (most common when purchasing rugged devices) to buying direct from an original equipment manufacturer (OEM) or mobile operator. Shop around for the best options and pricing.

Decide in advance if you want to purchase devices that are locked or unlocked. If it doesn't matter to you, then buying a locked phone may make it easier to secure the device. Plus, it can be difficult to ascertain whether your optimal devices are available in unlocked form. That said, buying unlocked devices gives you more choices when it comes to mobile operators, and it can be helpful for companies that have employees who travel internationally.

APP TESTING

You already know that handing out devices without proper configuration doesn't make for smart business. Make sure the apps that your company uses are also ready to go on the devices before you distribute them. Conduct tests to see that apps are properly connected to any backend systems, that they're storing data appropriately and securely, and that all the permissions are configured so that your employees can easily log on and access what they need to be productive.

If you have a BYOD program and support a range of platforms and devices, you may find that app testing can quickly become complicated and costly. Use logs to discover which devices, platforms and operating system versions are in use within your BYOD population, and start by catering to the largest percentages. You may want to run tests on both older and newer device models to really see what works.

KEEP UP TO DATE

Even after your devices have been disseminated, you can't sit back and relax. Those devices and the apps on them will need regular updates. If you're using an MDM or mobile application management (MAM) solution (or, better yet, a combination of the two), those updates will be easier to handle because they can be centrally managed. You'll also have the ability to blacklist rogue apps that pop up after deployment.

TAG – YOU'RE IT

One of the troubles with mobile devices is that they're, well, mobile, which means that they can easily wander off and become lost. Many companies keep a handle on roaming devices through asset tagging, in which each device gets a unique ID number that's recorded in a central database. It's possible to add radio frequency identification (RFID) technology to your asset tracking system to help locate devices.

COVER YOUR ASSETS

Even if they're tagged, it can be tough to track all those mobile devices, especially if you have a BYOD program. Proper asset management is key to maintaining your mobility investment. There are plenty of asset management systems out there that will provide you with reports about general inventory, which user has which device, how many licenses you have and when they expire, your wireless usage, device histories and so forth. With this information at your fingertips, you'll be able to control costs and plan for future investments.

THE MAINTENANCE WINDOW

You strive to avoid downtime with your mobile devices, but it does happen. Finding a fast way to repair or replace devices calls for comprehensive depot services. Companies can either establish their own mobile device depot or rely on an outsourcing partner to deliver depot services. Either way, employees with problematic devices will receive an immediate replacement and can get right back to work.

THINK GLOBALLY

If you have an international company, you'll need to do a bit of additional planning when taking on a mobile device deployment. For instance, if you're purchasing your devices from a single source, make sure that those devices are equipped for all the languages your employees need. You'll also need to find a mobility service provider that can handle your global scale. You'll want a partner that can provide comprehensive wireless coverage and that also can offer additional services that aren't platform-specific and that don't just skim the surface but truly provide full care for your mobile environment.

SO LONG, FAREWELL

Sad to say, at some point, your devices will reach the end of their usable lives. When that happens, you need to have a plan in place for how to dispose of them. If you've leased the devices, it's an easy path: You'll hand over your old devices and, most likely, sign up to receive new ones.

If you did not lease your devices, you'll need to properly retire or securely destroy them. Some companies provide disposal services that offer a partial refund for equipment that still has value. If your devices are no longer worth anything, look for green recycling programs or, if necessary, secure destruction, where devices are either shredded or wiped using a government-approved standard.

Need help with strategic mobility planning or getting your mobile apps decisions in order? We've got you covered.

Mobile Security

HOW TO DETERMINE WHICH PATH YOUR MOBILE SECURITY STRATEGY TAKES

Just as you can't safeguard your company's devices without proper security planning, you also need a plan for protecting apps and content.

PLAY IT SAFE: HOW TO DETERMINE WHICH PATH YOUR MOBILE SECURITY STRATEGY TAKES

Like it or not, there are people out there with malicious intent, and employees can be inadvertently careless. Just as you can't safeguard your company's devices without proper security planning, you also need a plan for protecting apps and content. Taking a three-pronged approach is the key to successful mobile security management. But before you consider the software solutions, policy settings and other tactical elements that make up your mobile security package, you need to identify how your company and your employees use their devices and how far you need to go on the security trajectory. Here's a sampling of areas to consider.

REGULATORY RIGMAROLE

Every company has its own standards for security, but some industries require companies to jump through more hoops than others. The world of mobility puts companies at greater risk of being out of compliance with regulations. Businesses that process credit cards are subject to the Payment Card Industry Data Security Standard (PCI DSS), healthcare organizations need to make sure that they stay compliant with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and publicly held companies must adhere to the Sarbanes-Oxley Act of 2002 (SOX). These are the biggies, but there are other, lesser-known regulations to be aware of. Make sure that you know your industry requirements as they pertain to mobile devices, apps and content.

Even if your company is not subject to stringent industry regulations, it is still a best practice to set security policies as though it were. After all, regulations are meant to help companies determine which information is considered sensitive, who should have access to it and under which circumstances, and how to respond if that information is compromised.

STAY FLEXIBLE

Security can be a double-edged sword. If you completely control your mobile devices, apps and content, you'll limit your employees' productivity. But if you give employees too much freedom, you're more likely to experience security breaches. It's best to determine where to draw that magic line for your company, your employees and your data. Also, because things change so quickly in the mobile world, it's smart to implement security policies that won't prevent your business from adapting down the road.

TAKE INVENTORY

Many of the platforms, devices and apps in your mobile environment already have security features that provide protection while others may not. Find out the details about all the components that make up your current environment, and determine which ones have adequate native protection.

EVALUATE BYOD

By now, you probably understand the benefits of bring-your-own-device (BYOD) programs. Unfortunately, BYOD programs do present their own security concerns. One of the challenges of BYOD is that security responsibilities can be distributed between the company and its employees. Some companies alleviate the problem by taking on the responsibility for mobile security. They use company-managed gateways to maintain consistent control over data access and storage at the policy level. Even without those gateways, companies need to have baseline security requirements for BYOD that include enhanced password controls, data encryption, the ability to lock devices after a certain number of unsuccessful password attempts, and remote lock and/or wipe features.

Privacy is another consideration when it comes to BYOD programs. In a survey of enterprise workers, most were concerned that BYOD would "transform IT from helpful business partner into an Orwellian Big Brother keeping round-the-clock tabs on all device activity." Lots of companies use tracking software to help with mobile device security, but the majority of workers feel that tracking – either their devices or the websites they visit – invades their privacy. You'll need to establish concrete policies and clearly communicate with employees so that everyone knows to what extent your company monitors devices.

HANDS-ON OR HANDS-OFF?

There's a lot that goes into properly securing any infrastructure, let alone one that includes devices that can be taken anywhere. Although IT departments have plenty of options to choose from for mobile security software, many are overwhelmed by the rise in mobility. As mobile technologies evolve, the process of securing devices, apps and content becomes more complex.

Some IT departments take on the challenge of protecting their mobile infrastructure, while others choose to rely on partners who offer mobile security expertise. If you opt to work with a partner to secure your mobile environment, find one that has experience in securing multiple platforms and in addressing the entire mobile lifecycle so that you don't run into roadblocks later.

DID YOU KNOW?

Mobile applications and services are overtaking the key activities that we used to do on the Internet. Mobile is an increasingly important part of any company's marketing strategy, and developers think mobile first when they design new Internet applications. In 2015, the app economy – the revenue driven through mobile apps and related activities – is expected to reach $100 billion.

BETTER THAN A SECURITY BLANKET: WHICH COMBINATION OF SOFTWARE SOLUTIONS IS RIGHT FOR YOU?

The first wave of mobile security software focused on the devices themselves. Now the focus has expanded to include mobile apps and content. Combining mobile device management (MDM) software with mobile application management (MAM) and mobile content management (MCM) software is most effective. The trick is to find the right balance among the three software types so that your mobile environment continues to run effectively.

MDM: KEEP DEVICES SECURE

MDM software focuses on centralized lifecycle management, but many features that fall under the device management category are also relevant in the security realm. For example, if you can use your MDM solution to update applications, you can use that same update capability as a way to reduce the vulnerability of your devices. MDM solutions help you enforce security policies and manage non-compliant devices by applying security measures, like blocking access to data or removing data from the devices. You can use MDM software to apply acceptable-use policies to devices, ensure that devices have the mandatory security settings in place, and issue devices with certificates for access. You can also enforce whitelisting and blacklisting of apps, disable unauthorized native apps and audit device settings to detect risky or potentially malicious activity – all good steps toward maintaining a secure mobile environment.

MAM: PROTECT APPS

As mobile apps become more relevant in the enterprise, MAM software is gaining popularity. And for good reason. MAM software helps ensure that mobile apps are free of malware and viruses, and it protects mobile environments by controlling access – only certain users can access particular applications on particular devices. These software packages can transparently install missing whitelisted apps, such as spam filters or firewalls, which means that you don't have to wait for employees to install and configure security apps.

You can use MAM software to track app downloads and usage. You can also use it to push updates for enterprise apps and remind your employees to install updates for non-corporate apps, thus keeping devices compliant with your security policies. When combined with the right MDM solution, MAM software can play a valuable role in securing mobile apps.

MCM: SAFEGUARD DATA

MCM deals with the data that's in use on mobile devices. By using MCM capabilities, your employees can securely share, collaborate on and send documents, presentations, videos and more. MCM strategies help establish a secure container around sensitive data, encrypting it and allowing only approved applications to access and distribute that data. Although still evolving, MCM solutions are expected to become more useful as integration improvements and the development of industry standards make it easier for devices and apps to recognize the protections placed on data.

BUT THAT'S NOT ALL

In addition to the "big three" in mobile security solutions, consider these other areas of opportunity:

Secure access. If your employees only use their devices for email, the security features (like Exchange ActiveSync) associated with your email systems are probably just fine. However, you probably need greater levels of authentication, so check that you have strong authentication to the network, encrypted tunneling capabilities and a host-integrity-checking capability that restricts access based on a user's security state.

Threat protection. As more people rely on their mobile devices, antimalware protection for mobile platforms has become increasingly important. Look for a robust grouping of web security capabilities that examines content from every possible angle to detect new threats.

Data protection. Embedded data loss prevention (DLP) capabilities in your email and web security gateways will control the data that can get to mobile devices in the first place. Mobile DLP functionality helps keep data from being exposed, whether accidentally or maliciously.

Mobile application reputation services. You can take advantage of several services that integrate with the major MDM vendors to provide risk assessments of applications. You can use the information from these services to perform quarantines, update for compliance and receive alerts if they detect vulnerabilities.

DID YOU KNOW?

Fifty percent of companies surveyed allow all corporate-owned devices to access social media sites and use related apps; 31 percent limit that access to certain departments. Just 19 percent ban it completely.

Forty-six percent feel only moderately confident that their mobile security controls are effective at protecting data.

Forty percent worry about users forwarding corporate data to cloud-based storage services.

THE NITTY-GRITTY: CONSIDER THESE SECURITY ELEMENTS, MEASURES AND PROCESSES

Aside from the planning that goes into your mobile security strategy and the software solutions that play a role in protecting your environment, the following mobile security methods and considerations may also work for your company.

Dual personas. The idea behind dual-persona devices is that two separate sets of usage controls exist within a single mobile device, which keeps personal and business information in separate buckets. This applies especially in BYOD scenarios. Not all devices are able to offer this dual-persona model, so look for that sort of mobile unified communication as you assess devices and providers.

Secure single sign-on. Secure single sign-on is fairly common in the desktop environment, and it is slowly becoming the standard in the world of mobility, too. By making it possible for users to gain access to all their apps and content through secure single sign-on, companies avoid the need for employees to remember multiple URLs, user names and passwords – yet apps and data remain protected. Users are authenticated once and then have one-click access to authorized apps, which keeps them productive and saves time for your helpdesk staff because users need less assistance with routine access-related issues.

Containerization. Your employees might be cautious, responsible users, but they could still accidentally put company content and systems at risk by downloading unsafe applications or tapping into unprotected personal content. Containerization separates business and personal content and makes it possible for IT staff to control business content without affecting personal information. App containerization technology provides each managed app – and its data – with its own secure "container."

Mobile operating system security. Different mobile operating systems have different security capabilities. It can be helpful to compare access control options, such as file system encryption availability, type of SD card encryption and security patch flow. Knowing how these mobile operating systems differ may have an impact on your purchasing priorities.

Security analytics and predictive intelligence. Addressing big data is one of the current technology trends, and that big data can help you shore up your mobile defenses, too. If you apply business

DID YOU KNOW?

Many employees, especially in a BYOD environment, treat their businesses and personal practices the same:

- *22 percent install software that can find the phone if it's lost.*
- *14 percent install an anti-virus app.*
- *11 percent use a PIN longer than 4 digits, a password or unlock pattern.*
- *8 percent install software that can erase the data on the phone.*
- *7 percent use security features other than screen lock, such as encryption.*

intelligence to your mobile environment, you can sniff out abnormal behavior and administer real-time security compliance protocols for devices that access sensitive corporate data.

Wi-Fi risks. One often-overlooked area of mobile security involves Wi-Fi access. Most mobile device platforms make it easy to connect to a previously used Wi-Fi access point, but it's simple to impersonate those connection points and attack connected devices. Deploy configuration profiles with corporate Wi-Fi settings, with the highest validation enforced, and encourage employees to use private, rather than public, certificates.

KEEP IT CURRENT

Mobile security isn't a set-it-and-forget-it deal. Once you have a plan in place, you have to keep it current or you'll put your company in jeopardy as security threats and employee needs change. Take time on a quarterly basis to assess new risk factors and indicators that may cause you to adjust your policies, device settings and other aspects of your mobile environment.

Need more assistance working through the challenges that mobile security presents?

Take a look at our MDM white paper and BYOD policy template.

SOURCES

1. Trusted Mobility Index
2. Companies Focus on Mobile Device Rollout While Overlooking Security, IFS Study Reveals
3. Forbes, What Drives the Mobile App Economy?
4. InformationWeek, Mobile Security Forum
5. CNBC, Most Americans Don't Secure Their Smartphones

FOLLOW US:

Mobility Management

HOW TO ADDRESS MANAGEMENT CHALLENGES IN A MODERN MOBILE LANDSCAPE

When done correctly, enterprise mobility leads to increased user productivity, better customer service and faster decision making. Getting it right, however, is no small task.

HOW TO ADDRESS MANAGEMENT CHALLENGES IN A MODERN MOBILE LANDSCAPE

Mobility management can be something of a catch-22. When done correctly, enterprise mobility leads to increased user productivity, better customer service and faster decision making. Getting it right, however, is no small task. In addition to supporting those business drivers, IT departments must carefully manage mobile devices, apps and content to protect against data breaches and meet regulatory mandates. To do so, they need the proper strategy, tools and mindset.

BRACE YOURSELF FOR OUTLYING DEVICES ("BYOD")

The bring-your-own-device (BYOD) phenomenon has transformed the way companies think about mobile devices and mobility management. BYOD gives employees choices, which means they can work with familiar, comfortable devices instead of the specific devices prescribed by their employers. At the same time, BYOD is likely the greatest threat to security management. Employees may not adequately protect their devices, putting those devices at a higher risk of exposure to malware. Factor in the challenge of separating corporate and personal apps and content, and you have a recipe for potential problems.

FREEDOM TO APP

The concept of BYOD is no longer revolutionary, and most companies are at a point where they expect BYOD situations. Many are finding ways to secure devices and manage only corporate apps and data, keeping employees' personal information in a separate bubble. Enter BYOA, the bring-your-own-application trend, which is expected to be the next wave of consumerization. More and more, employees are connecting to cloud services over their corporate network and downloading third-party apps, pushing IT departments to find ways to manage the mobile app environment.

Done well, BYOA initiatives can produce the same positive benefits as BYOD programs – namely, productivity. Employees who use familiar apps are more efficient and require less training from a corporate standpoint.

DID YOU KNOW?

If you think CIOs have concerns about BYOD security strategy, consider the next emerging trends: bring your own applications (BYOA), bring your own network (BYON) and bring your own cloud (BYOC). These are forcing IT teams to reconsider current policies, revitalize their mobile strategies and craft an IT roadmap for the future of mobility.

THE CHANGING APP LANDSCAPE

Of course, it's not just users who are evolving. Developers are creating mobile apps that revolve around business process re-engineering. These sophisticated apps behave more like business users need them to – taking workflow processes, collaboration needs, role-based operations and user locations into account. The result? Apps are becoming more mature for effective use across time zones, corporate security methods and provisioning mechanisms. To monitor app usage, IT departments will need to adjust by using dynamic policy rules that change depending on app behaviors, alerts and updates.

DIVERGING DEVICES

Emerging device form factors pose an additional challenge for IT departments, and the changing combinations of carriers, features, operating systems, configuration options and connectivity services add layers of complexity. Plus, you can no longer assume that one employee equals one device, because many want to use their smartphones, tablets and other mobile devices for work purposes.

If you get bogged down in all the variables, service to your users may suffer. And if employees can't get the support they need from the corporate helpdesk, they'll look to another (less-reliable) source or end up stymied and frustrated, negating the benefits of having a mobile infrastructure in the first place. Fortunately, proper management can address these challenges and provide you with the efficiency gains and user satisfaction results that mobility can deliver.

DID YOU KNOW?

Apps are becoming more mature for effective use across time zones, corporate security methods and provisioning mechanisms.

ABRACADABRA: HOW TO WORK YOUR MANAGEMENT MAGIC TO CREATE THE OPTIMAL MOBILE ENVIRONMENT

When it comes to managing mobility, you have to balance expenses, wireless network management, device/app/content management and possibly even virtualization. With so many factors to consider, it's critical to get everyone on the same page; managing a mobile infrastructure is challenging enough without working at cross purposes.

FIND A FLEXIBLE FOUNDATION

To make sure that everyone is working toward the same goals, establish a management plan that prioritizes investments, ensures an efficient mobile infrastructure and helps you take action on mobility mandates without jeopardizing security. A cross-team steering committee can help with the mobility management roadmap. Keep in mind that your plan needs to be structured enough to guide you now and flexible enough to avoid limiting you down the road.

ALPHABET SOUP: MDM, MAM, MCM, MIM

Finding the right combination of software solutions can ease the burden when it comes to managing your mobile infrastructure. Remember to take a holistic approach to management, because you'll need to cover devices, apps and content. Start by researching the features, benefits and weaknesses of each potential solution component. You'll likely want a blend of mobile device management (MDM), mobile application management (MAM) and mobile content management (MCM) – sometimes referred to as mobile information management (MIM) – solutions.

MDM. Not long ago, MDM software was considered the solution for all enterprise mobility needs. With the rise of enterprise mobile apps and the growth of the BYOD movement, however, MDM solutions just aren't enough on their own. A solid MDM solution is now considered an important component of a good mobile management plan; your MDM solution should include capabilities for mobile asset inventory, device provisioning, software distribution, security management, data protection, and monitoring and helpdesk support, among others.

MAM. Covering many of the gaps left by MDM solutions, MAM solutions focus on controlling access to specific applications. Look for MAM solutions that also offer mobile software delivery, software licensing, app configuration, app maintenance, usage tracking and policy enforcement.

MCM. Even with MDM and MAM solutions on your side, you still face a risk that your sensitive data will make its way beyond the walls of your corporate network. MCM solutions should include device-

agnostic capabilities for data encryption, compliance management and secure data distribution and sharing, all of which prevent the exposure of data through improper dissemination.

THE NEXT GENERATION: MOBILE LIFECYCLE MANAGEMENT

If it seems to you as though all of these management solutions are a lot to manage, you're not alone. There's a trend toward combining MDM, MAM and MCM into an all-inclusive platform, known as mobile lifecycle management (MLM) – or enterprise mobility management (EMM). Most of the time, MLM and EMM platform solutions blend mobile expense management with mobile device/app/content management to help you control the entire device lifecycle. They help you manage mobile endpoints, apps and data securely, all while simplifying that management and often reducing the overall cost of operating your mobile infrastructure.

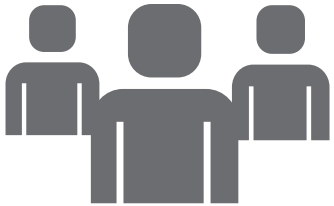
IN PARTICULAR...

There are a few solution elements that you should consider as you seek mobile management nirvana:

Enterprise app stores. Many MAM solutions include enterprise app store capabilities, which give you a way to offer company-sanctioned applications in a convenient, easy-to-manage location. Employees can find and download what they need, and your IT staff can control the environment to avoid application overload. A well-run enterprise app store will help you better manage the app lifecycle and enforce your app policies.

Dynamic policies. As discussed, the behavior of the next generation of enterprise mobile apps will depend on a lot of variables. To help manage, monitor and secure those apps, IT departments will need to incorporate dynamic policy rules that change instantly based on the applications' behaviors. Sounds complicated, but you're in luck – many MAM solutions come with this kind of baked-in flexibility, removing the need for IT staff to constantly monitor employee app usage. Instead, they receive updates and alerts dynamically. Also, any policy changes can be automatically pushed to mobile users the next time they log on to the corporate network.

Network access control. Long a tenet of desktop management, network access control (NAC) is a way to strengthen network security by limiting the availability of network resources to endpoints that comply with a set security policy. As employees use more mobile devices for work, companies are turning to NAC solutions to protect their internal networks from rogue devices and from devices that aren't fully managed. Several NAC solutions now take mobility into consideration. For instance, it's possible to configure your solution so that corporate-managed devices have different access rights than BYOD devices. It's



If it seems to you as though all of these management solutions are a lot to manage, you're not alone.

also possible to tie your NAC solution directly into your MDM solution for easier management.

Existing IT infrastructure. Your mobile environment doesn't exist in a vacuum, so it's important that you take a look at the rest of your IT infrastructure to see how it can lend a hand when it comes to mobility management. For example, by using Active Directory Domain Services and either in-house or hosted certificate services, you can leverage more automated processes and higher security levels on the mobile side.

Cloud services. By now, many organizations recognize that using the cloud can simplify infrastructure management and allow services to easily scale. By using the cloud for mobility management, you can operate from a centralized hub, usually through some sort of web-based administrative console, where you can manage numerous apps and provide your employees with an integrated experience.

Application risk management. If you set up your MDM solution a year or two ago, you may have been pondering how to set up and maintain white and black lists of applications that you want to look out for or prohibit. Now several companies, such as Appthority, have tie-ins with MDM solutions to facilitate that upkeep and also raise the level of automation, so you could easily quarantine or block suspect devices based on multiple risk factors.

Lifecycle services. Sometimes it just works better to leave management to the experts. If you'd rather focus on your core business and make your mobile environment more predictable, consider finding a service provider that can deliver agnostic mobile lifecycle services.

REAP THE REWARDS: WHY A MULTIDIMENSIONAL MOBILITY MANAGEMENT STRATEGY MATTERS

The purpose of enabling a mobile workforce is to increase employee productivity and improve customer service, both of which benefit your business. Without a comprehensive, strategic approach to mobility management, you could miss out on all the gains that mobility, when done right, can deliver.

To learn more about enterprise mobility – from strategy to deployment – check out the Enterprise Mobile resources page.

SECURE DATA

Data protection is critical to companies. After all, IT security budgets are increasing everywhere. It's no different for data that lives or is viewed on mobile devices. Taking advantage of MDM, MAM, MCM and NAC solutions as part of your mobility strategy can help you maximize data protection at the device, app and network levels. By doing all that you can to safeguard content, employees will have the information they need at their fingertips without being in a position that could put the company at risk.

AN EFFICIENT, EFFECTIVE IT DEPARTMENT

A fancy new mobile device can have employees tiptoeing through the proverbial tulips and leave IT staff weeping softly in a corner. A mobile infrastructure can be beneficial for employees, but it also places a heavy burden on IT staff, especially because the mobile landscape is changing so rapidly. If you can standardize endpoint management across device types and platforms, you'll be in a good position to embrace trends and respond positively to user demands without overtaxing your IT staff or breaking the bank. Holistic management will help you address trends like fragmentation in the mobility market, BYOA and a workforce that juggles multiple devices.

HAPPY, PRODUCTIVE EMPLOYEES

The goal of mobility is to make it possible for employees to work whenever they want from wherever they happen to be. Businesses that optimize for mobility can empower employees to safely use their personal devices for work and make it easier to remotely access and share documents on the go. As a result, employees can boost productivity from anywhere, respond more quickly to customers and still relax with a game of Angry Birds at the end of the day.

SOURCES

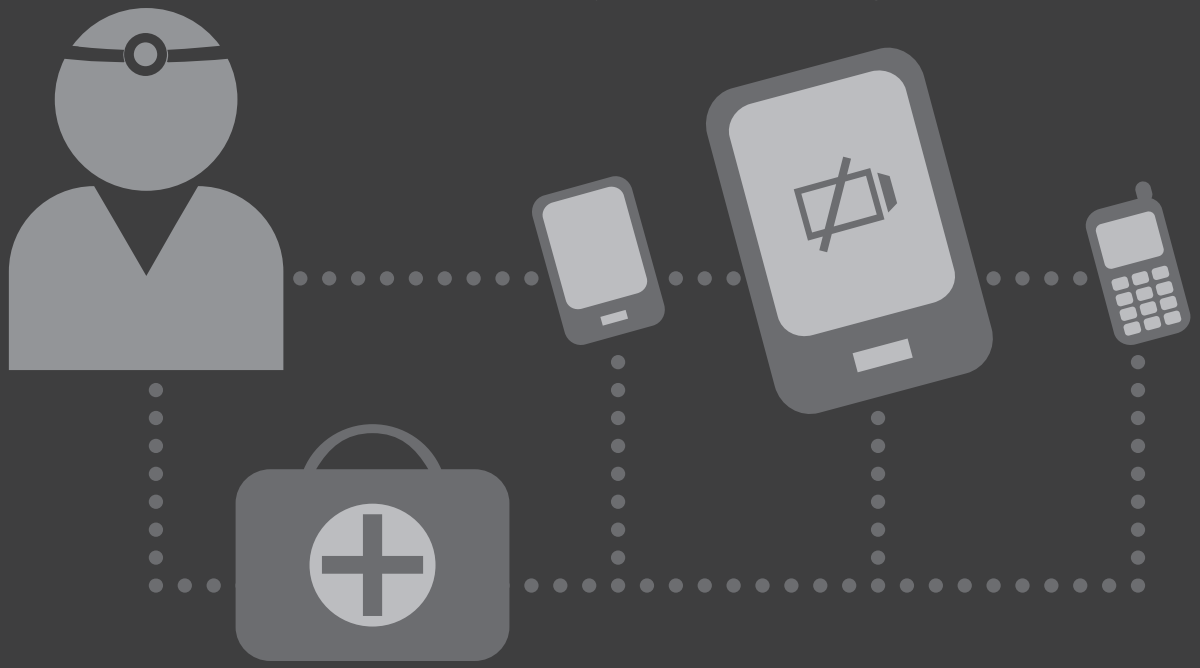
1. The Impact of Mobile Devices on Information Security: A Survey of IT Professionals
2. Mobile Life Cycle Management Takes Charge of BYOA
3. SearchCIO, Planning for the Future of Mobility: A BYOD guide for enterprise CIOs
4. Statista, Mobile Device Management Revenue Worldwide

FOLLOW US:

Mobile Workforce Support

WHY THE RIGHT SUPPORT SETUP MATTERS

If your employees can't use their mobile devices properly, your company isn't reaping the benefits of your mobility investment.



BACK A WINNER: WHY THE RIGHT SUPPORT SETUP MATTERS

It's a reality – just like PCs, mobile devices can malfunction, experience glitches and stop working altogether. Responding swiftly and correctly to those issues is just as important as responding to problems with employees' desktop computers. After all, if your employees can't properly use their mobile devices, your company isn't reaping the benefits of your mobility investment.

The primary purpose of allowing employees to use mobile devices for work is so that they can use them whenever and wherever business takes them. Unfortunately, this creates challenges for a 9-to-5 support staff, especially if those staff members aren't well-versed in all things mobile. Employees who experience technical difficulties with their mobile devices while outside of normal business hours, or when no one in IT is available to help, have few options but to wait. Delays like this put a drain on productivity and can lead to sagging workforce morale.

WHAT COULD POSSIBLY GO WRONG?

Many IT departments are under the impression that as long as employees avoid damaging a device, it's all good. It is important to remember, however, that devices can also be lost, stolen or improperly configured, all of which have an impact on productivity.

Plus, it's not only the device that needs support. Employees may have trouble when their enterprise mobile apps get updated, or they may be unable to access data on their mobile devices. As enterprise mobile apps become more prevalent, helpdesk staff may need to devote more time to learning the ins and outs of mobile apps that are critical for user productivity.

MISSING KNOW-HOW

Because mobility is relatively new from an enterprise standpoint, many IT departments treat mobility support with lower priority than desktop support. Most enterprise IT administrators are either too busy or lack the specific domain training and expertise to properly support mobile devices. That support is made more difficult by the fact that most enterprises must address an ever-expanding range of devices, apps and operating systems. Successfully helping employees sort out issues with their mobile devices requires a certain set of skills, so IT managers should make sure that helpdesk staff members have the necessary training to keep employees up and running.

Bring-your-own-device (BYOD) programs further complicate matters at the helpdesk because they require support staff who are ready and able to deal with issues on both personal and corporate devices. If your employees are using personal devices for work, they'll need support. Determining the scope of support you'll offer can be a challenge.

HIGH PRIORITIES, HIGH STAKES

As mobile functionality grows even more useful, employees will increasingly consider their devices "business-critical." When you – or mobile device providers or enterprise mobile app developers – make changes to the mobile landscape, you need to anticipate an uptick in mobile support needs. It's critical that you plan for providing that extra help. Otherwise, you'll overburden IT staff members and force them to set aside other important projects. Proper planning (and staffing) for mobile support will keep your employees productive and your helpdesk effective.

MOBILITY DOUBLE STANDARDS

Employees and IT departments don't always see eye to eye on the importance of mobile devices when it comes to maintaining productivity. For employees, waiting more than a day or so for a new handset, charger or device may be unacceptable. For an IT department, providing the right accessory or device in a timely manner might be costly, if not impossible, due to procurement limitations. While the norm in the desktop world may call for immediate service, that doesn't always extend to mobility. Keep in mind that, to some employees, having a viable mobile device may be even more important than having a fully operational PC. Employees often feel as though their hands are tied without their mobile devices, causing them to revert back to the old (read: less efficient) way of doing business.

DID YOU KNOW?

Employees and IT departments don't always see eye to eye on the importance of mobile devices when it comes to maintaining productivity.

PUT THE "PRO" IN "PRODUCTIVITY": HOW TO STRUCTURE YOUR MOBILE SUPPORT INFRASTRUCTURE

Perhaps the most important element of mobility support is speed. Responsiveness is the name of the game. Your employees may be working 24x7, so they need around-the-clock support, too.

TRAVELING THE GLOBE

If your employees bring their mobile devices on business trips, you'll need to be right there with them. Whether you set up support centers in different geographies, rely on outside help or provide assistance virtually, make sure your employees have an accessible place to turn.

SHARED RESPONSIBILITIES

As BYOD and bring your own app (BYOA) become more widespread, employees and IT departments need to acknowledge that helpdesks often now support both business and personal activities on mobile devices. With the convergence of applications and data, even contact lists, pictures, music and games may have to be part of the support equation. If you're not planning to support everything, be upfront about it – define policies for the specific areas that you support, and be clear about which apps and data are allowed on corporate-managed devices.

STANDARD ISSUE

Like helpdesk services for any other business area, your mobility support should include a tiered structure for fastest service on the most common issues. Think through your processes and create workflows to make sure you're covering all your bases. You also should establish standardized timelines for device repair and replacement. Set expectations for your users, bearing in mind that immediate or next-day replacement is often considered a must-have level of service.

TEACH A PERSON TO FISH

Keeping helpdesk calls to a minimum makes it possible to focus on the employees who really need your assistance, but how do you prevent people from calling for non-critical reasons? Empowering employees through self-service is a good first step. Develop a knowledge base for the device – and make sure that how-to and FAQ documents live on the device itself for easy access. You can also include direct links to mobile support content in your app store. Automation is another option for simple operations, such as enrolling devices or handling day-to-day tasks associated with mobile device use.

WAIT, THERE'S MORE!

Click here for additional information on mobile support solutions.

KNOW THE ROPES: WHAT MAKES MOBILE ENVIRONMENTS UNIQUE

In many ways, supporting a mobile environment is more complicated than supporting desktops and laptops. You have less control over just about everything, and there are more variables to anticipate and address. But awareness and preparation on your part can mitigate worry and provide a mobile environment that promotes corporate success.

THE FUNDAMENTALS

Phones, tablets and ruggedized devices have their own sets of considerations when it comes to support. Be aware of the areas requiring support for each device type:

Phones. Communication is key, and it can be in the form of voice, text and email, all of which can apply to business and personal uses. Next, think about connectivity and how issues with carriers, corporate networks and home and public Wi-Fi can crop up. Finally, consider which personal activities (entertainment, photography, gaming) you will support.

Tablets. The primary issues for tablets center around applications, so you need to know how to support at least the most frequently used business, education, proprietary and multimedia apps. Again, you'll need to deal with issues related to connectivity and personal activities, but those are typically secondary to apps when it comes to tablet use.

Ruggedized devices. Ruggedized device users can experience some of the same challenges as employees who use regular phones and tablets. They may also need help with scanning and printing capabilities, along with proprietary line-of-business apps.

CONTROL FREAKS

Like it or not, you can't always anticipate issues with your mobile environment because there are so many moving pieces at work. Wireless carriers, for instance, play a large role in keeping your employees productive and happy, so you have to take them into account. Carriers have their own coverage areas, data plans, warranties and liability policies, all of which affect support.

The good news is that carriers also have their own helpdesks, each with its own skill set and service-level agreements. They have policies and procedures for dealing with moves, changes, additions and deletions (MCAD), so be sure to take advantage of their services.

TOP SIX

You never know when an employee will accidentally disable or damage a mobile device, whether it's drowning it, smashing it or overheating it. Issues can run the gamut, but you can serve most of your users if you focus on the most likely candidates when it comes to mobile support:

Email access. This includes corporate and personal aliases, settings (server names, IP addresses, etc.) and sync/configuration issues.

Connectivity. You may hear about problems with call quality, carriers (not enough "bars") and public and private Wi-Fi.

Power. This includes waning battery life and charging difficulties.

Passwords. Password resets can become the bane of a helpdesk staff's existence, but they're a reality.

How-to information. New devices, apps and operating system updates can cause confusion and result in support calls.

Device replacements. When something goes terribly wrong, sometimes only a new device will do.

TECHNICIAN'S WORKSHOP

Speaking of device replacements, make sure you offer depot services so that you can quickly deploy a new device when an employee needs one. Keep in mind that batteries, chargers, headsets and other accessories all qualify as must-have items.

STOP, THIEF!

Desktop and laptop computers do get stolen from time to time, but making away with a mobile device is even easier. Mobile device management (MDM) locator tools can help you find stolen or lost devices, but you should also have policies and processes in place for device wipes and device locks. And it's important to close the loop by filing police reports and checking carrier policies about those lost or stolen devices.

GOING PRO

It may be that caring for your mobile infrastructure is more than you can or want to take on. By working with a mobility services provider, you can streamline support and keep your IT staff focused on your own business priorities. For many companies, outsourcing mobile support is cost-effective, helps mitigate risk and lends itself to flexible staffing. Ultimately, mobile employees receive faster, better service so that they can get back to adding value to the business.

SERVICE PROVIDER CHECKLIST

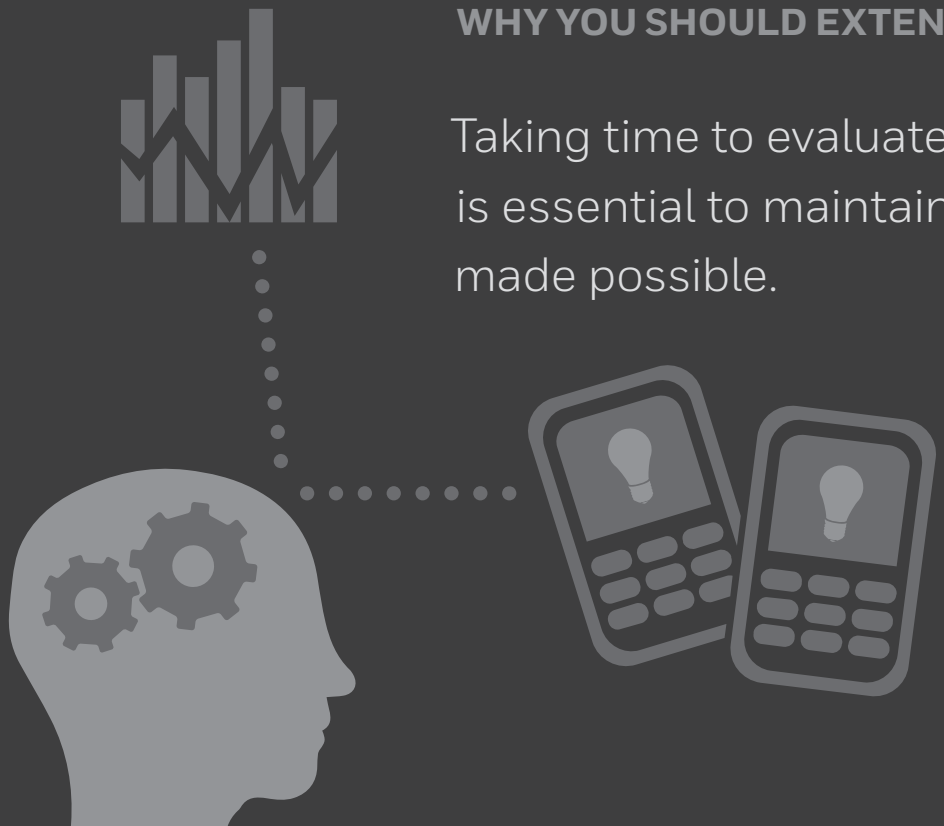
If you decide not to go it alone, you'll need to find a trusted partner who can help provide the level of support that your employees deserve. Look for one who:

- *Offers 24x7 service*
- *Has international capabilities*
- *Can advise on policy development*
- *Creates helpdesk workflow processes*
- *Provides depot services*
- *Has experience with a range of device types*
- *Can handle any issue related to either hardware or software, regardless of operating system*
- *Keeps up with changing carrier coverage areas, data plans, warranties and liability policies*

Mobility Intelligence, Monitoring and Analytics

WHY YOU SHOULD EXTEND BUSINESS INTELLIGENCE INTO THE MOBILE SPACE

Taking time to evaluate the effectiveness of your mobile environment is essential to maintaining the success that your initial planning has made possible.



GET SMART: WHY YOU SHOULD EXTEND BUSINESS INTELLIGENCE INTO THE MOBILE SPACE

For many organizations, mobile capabilities evolve from grassroots adoption; though not ideal, technologies often enter an organization before its IT department is ready for them. As mobility grows more pervasive, it becomes a mission-critical system, worthy of regular assessment. Carefully and consistently reviewing the performance of your mobile environment will help you make more strategic decisions about mobility.

MEASURING SUCCESS

Many companies focus on the cost ramifications of mobile environments, but there are plenty of other considerations. By collecting data across the board, you can calculate compliance, security risks, application usage, remediation, user acceptance and other factors that are critical to assessing the value of your mobility investment. Without these monitoring processes in place, you might miss out on opportunities to tweak or make wholesale changes to your environment that could have a positive impact on your employees, your customers and your bottom line.

ONE-HIT WONDER

Analyzing the ins and outs of your mobile environment shouldn't be a one-time occurrence. Identify trends over a period of time and try to understand the fluctuations. They may have to do with the use of a particular app, the number of devices that you manage or the level of helpdesk support necessary for your employees.

It may be easy to spot the factors that influence your environment – for example, an uptick in support calls may correlate to the rollout of a new mobile app. But there may be other variations that you'll need to delve into. For instance, if a specific office fields more support calls, could there be widespread connectivity issues in that area? Is a lack of user education and training to blame? Or do your helpdesk staff members need extra training themselves? Through careful analysis, small issues can be brought to the surface, and you can take appropriate steps to optimize your environment.

EYES ON THE PRIZE

To analyze your mobile environment effectively and come up with actionable information, you'll need to think back to your original mobility strategy. What were your business and technical goals? How do you know if you're meeting them? Make sure that the data you collect reflects what you need to know about your mobile infrastructure. Otherwise, you'll monitor simply for the sake of monitoring, which isn't a smart use of time or resources. Only by comparing your data to your original plans will you know if your mobile infrastructure is delivering the value that it should.

OBSERVED BEHAVIORS: HOW TO KNOW WHAT'S REALLY GOING ON IN YOUR MOBILE ENVIRONMENT

It's nice to know how many support calls came in last month or how many apps you offer in your enterprise app store, but those bits and pieces of data don't give you the overarching view that you need for truly helpful analysis. Take a 360-degree view of your complete environment and all its moving parts so that you can better understand how mobility really works at your company and make informed decisions about where to spend, where to save and how to get the most from your mobile investment.

PUT YOUR EGGS IN ONE BASKET

So you're on board with the idea of a holistic view, but how do you go about gathering that comprehensive data? Even if you have a useful mobile device management (MDM) solution in place, it won't give you all the answers. You'll need to tap into all the potential sources of information in your environment. A full enterprise mobility management analysis may include a synthesis of data from your MDM, mobile application management (MAM), security, asset management, support management and telecom expense management solutions.

THE HUNT FOR DATA

What kind of information should you be collecting from all these systems? Start with proactive and reactive real-time assessments of the state of individual devices or groups of devices. Consider these questions to help you get started:

- How many devices does my environment support, and what are they?
- Who uses them?
- Are all those devices active?
- Are all apps properly installed and current?
- Is security in place at the device, app and/or data level?
- When it comes to support, how many tasks (installs, troubleshooting, device wipes, device unlocks, password resets) have been completed in a given period of time?

CAP YOUR COSTS

Getting the biggest bang for your buck is often the first consideration in business analytics. That's certainly true when you look at your mobile environment, and mobile infrastructures often provide ample opportunities to reduce costs because the landscape changes so rapidly. Try to gain better control over roaming costs, and negotiate contracts with telecom operators by using best practices and lessons learned from other companies.

DEFINE BYOD SUCCESS

With a bring-your-own-device (BYOD) program in place, it can be difficult to know exactly what's going on with employee-owned devices, especially if you share management with your employees. Through proper monitoring, you can determine whether devices are enrolled so that you're protected from security breaches, and you can also gain big-picture information about your BYOD program. If you provide BYOD support, are you keeping track of ticket volume, problem areas and knowledge-base content? Are you providing user surveys to see if your BYOD program is successful? Are you getting negative or positive feedback at different levels? Are you providing the right forward-thinking BYOD strategy for your business?

TELECOM CONTRACTING BEST PRACTICES

Define your requirements. What are your capacity and throughput needs? What sort of geographic coverage do you require? How much redundancy is necessary?

Check providers' financials. Look at annual reports, industry ratings and recent articles.

Examine service offerings. Make sure you know which services are offered, how long they've been on the market and how satisfied customers have been with relevant services.

Check for minimum annual commitments and/or volume caps that can affect your pricing if your usage doesn't fall within a certain range.

Ask for a rate review clause so that you're not locked in to a set rate over an extended time period.

Ask for a rate stabilization clause, which assures you that your rate won't increase.

Set clear service-level agreements and contract terms. Gain an understanding of how you'll be credited if those terms aren't met.

Establish an escalation path. It's critical that you have a set communication route if your telecom provider is not meeting expectations.

Know your termination rights.

Manage telecom capacity like an asset in your inventory – review your services quarterly, if not monthly, so you can ensure that you're always getting the best deal.

KEEP IT SAFE

Proper analysis of your environment can help ensure that you're doing all that you can to safeguard your mobile infrastructure. It will keep you abreast of new mobile operating system releases and bug fixes. Important security practices also apply to mobile devices – keep them updated and patched to minimize known security risks. Do you view your mobile devices as endpoints and put the right solutions in place to safeguard them? Various network access control and security information and event management solutions now support mobile devices and can provide more valuable information. Review reports about security incidents – the number, the frequency and the severity – to see if you should change your policies.

CHECK YOUR GROWTH CHART

Keeping tabs on your mobile environment makes it easier to manage business growth (or contraction). Has the size of your organization changed since you established or last reviewed your mobile infrastructure? If your employee count has increased, are you now able to take advantage of any new economies of scale? On the flip side, if you've downsized, are you paying for devices and/or services that you no longer need?

KNOW YOUR APPS

As you continue to invest in off-the-shelf mobile apps and begin to develop your own custom apps, you need visibility into app utilization so that you can appropriately allocate your IT resources. After all, there's no sense in paying for the widespread licensing of an expensive app if only a few employees use it. If a particular app appears to be rarely used, IT staff can ask business groups to justify spending resources on it and can instead encourage spending on apps that are heavily used and more valuable to the company as a whole.

Your MAM solution should provide you with app-level data so that you can identify usage by app, platform and version to help you evaluate your app spending. You can also use that information to scale your number of licenses based on real-world utilization. That knowledge can help you avoid becoming out of compliance with your software license agreement and paying for licenses that you don't need. Plus, if you have a better understanding of app adoption in your organization, you'll be able to handle current and future app rollouts more gracefully so that your company derives the most value from your investment.

Click here to learn more about Honeywell's Mobility Assessment, which can provide your organization with:

- *A comprehensive analysis of carrier spend*
- *Detailed savings recommendations*
- *Information to validate ROI*
- *Savings of 15–20 percent*

HOLD THE PHONE: TELECOM EXPENSE MANAGEMENT

In an environment of both corporate-owned and employee-owned devices, employees have the freedom to use their preferred devices where appropriate, while employers maintain control of important assets where necessary. This type of mixed mobile environment can be beneficial, but it creates challenges regarding telecom expense management (TEM). Traditional TEM solutions use data from your corporate phone bill, which doesn't take into account all those devices that are enrolled through your BYOD program, so you end up having to cobble together data to determine your total mobile spend. Newer TEM solutions track corporate-owned and employee-owned devices in a single view, so you can continuously balance BYOD and corporate device costs together as part of a unified mobility strategy. In addition to consistent cost tracking, using a next-generation TEM solution can assist with enrollment management and improve visibility into your entire mobile ecosystem.

BEST SUPPORTING ACTOR

Mobility support is perhaps one of the areas that's easiest to analyze. But some companies fail to take in the complete support picture. In addition to the standard pieces of data, such as the number of devices under management and total helpdesk call volume, consider tracking and monitoring the following areas to get a better understanding of the support experience that you're providing:

- Anticipated versus actual call volume
- First-call resolution rate
- Abandonment rate
- Average speed to answer
- Average handle time
- Top call drivers
- Ticket origin (email versus phone call)
- Escalations
- Top callers
- Anticipated versus actual device depot volume
- Device depot service levels
- Device replacements by geography
- Depot inspection results
- Damaged device data by issue

A SCALE FROM 1 TO 10

Your systems – even taken as a group – can't provide you with all the information you need. That's where employee surveys come into play. You may see that employees aren't using a certain line-of-business app on their mobile devices. Why is that? Try asking them. Surveys can include questions about the devices that they like using most, the apps that they find most helpful, the gaps in your mobile infrastructure or in your mobile support that they'd like to see filled, etc.

AN OBJECTIVE VIEW

It's not always easy to make sense of the volumes of data that your various mobile management solutions produce. Some companies work with outside partners to get a comprehensive, unbiased view of their mobile environments. Outside vendors can aggregate data from your disparate systems and use their own analytics capabilities to make short- and long-term recommendations about managing mobility. Certain vendors can also help you validate potential software solutions so that you can make the right choices for your environment.

Conclusion

A mobile infrastructure requires diligence, from initial planning to ongoing monitoring and analysis. When handled right, your mobile infrastructure can yield the treasured triple play that most organizations strive for: greater employee productivity, increased profitability and reduced total costs.

A solid mobile infrastructure starts with a strategic approach. **Enterprise mobile planning** helps you focus on mobility goals that are tied directly to your overall business strategy, and it helps conserve costs and avoid duplication of effort.

The growing emphasis on enterprise mobile apps means that you should carefully evaluate your app needs. **Mobile application development** comes with a lot of decisions, and properly delivering, supporting and securing those apps can make a real difference in employee productivity.

Enterprise mobility deployment may sound simple, but all that configuration and securing of devices requires real know-how. Taking a close look at how to structure your rollouts (and thinking ahead about components and accessories) can have a huge impact on the adoption and long-term success of your mobile initiatives.

Although most organizations take the time to secure their corporate-owned mobile devices, the majority don't go a step or two further to consider how best to safeguard mobile apps and data. **Mobile security** requires a three-pronged approach, especially when personal devices enter the picture through bring-your-own-device (BYOD) programs.

Without ongoing mobility management, you won't get the value out of your **mobility investment**. Plenty of software solutions can help you manage mobile devices, apps and content. And a multidimensional management strategy will make it possible to protect your company's interests while keeping IT staff efficient and employees productive.

When something does go wrong, make sure you're ready to respond by thinking ahead about **mobile workforce support**. Up-to-date training for helpdesk staff, a clear understanding of support responsibilities for BYOD program participants, self-service components and depot services all contribute to keeping your mobile infrastructure up and running smoothly.

Tracking the virtues – and shortcomings – of your mobile environment is critical to long-term success. **Mobility intelligence, monitoring and analytics** help ensure that you're spending your budget in the right areas and enable you to make smart decisions based on real-world data.

For more information
www.honeywell.com/enterprisemobility

Honeywell Sensing and Productivity Solutions
9680 Old Bailes Road
Fort Mill, SC 29707
800.582.4263
www.honeywell.com

Follow us:

Essential Guide Ebook | Rev B | 01/16

Honeywell