# Every Business Is a Mobile Business

By Kevin Casey

Sponsored by:

ca technologies

# EVERY BUSINESS IS A MOBILE BUSINESS

## Overview

Whether you were at the forefront of the mobility era or are just now catching up—or, most likely, somewhere in between—you've already experienced first-hand the business impact of ubiquitous smartphones and tablets. From employees to customers, mobile devices spawned an explosion in new applications, data, support needs, security concerns, and other issues. They've reset expectations for organizational speed and flexibility. They've dramatically increased the surface area for potential security attacks. All this, and the mobile era is still just in its infancy.

We're now about to experience two new, related booms in mobility: the prevalence of wearable technologies, such as smartwatches and connected health monitors, and the Internet of Things (IoT), where everything from your car to your toaster to your **drinking glass** might be "smart" and connected online.

In other words, mobility will no longer simply mean a smartphone in every pocket and a tablet in every home and office. This trend presents serious opportunities for businesses and IT departments—and serious risks for those that turn a blind eye to the evolving mobility landscape. Every business is a mobile business these days, whether it realizes it or not. Customers expect a high-quality, secure mobile experience when doing business with you. Internal customers—the employees that keep your company up and running—likewise expect the rapid delivery and support of mobile applications that help them to better do their jobs and meet business objectives. Strategic organizations will implement forward-looking plans to best manage the effects the next waves of devices and applications will have on their businesses.

The old way of doing things—siloed teams working independently of each other, protracted development and testing cycles, reactive security approaches, slow bug fixes, and other processes born out of the premobile age—simply won't suffice in the always-on world of enterprise mobility.

A recent **InformationWeek story** on "frictionless IT" notes: "IT organizations are facing rising demand for faster development, thanks to the increased strategic importance of analytics, the Internet of Things, a mobile-equipped workforce, and increased expectation that business will be done digitally. Mobility is an essential part of the equation."

The mobility revolution requires better technology tools as well as new ways of thinking and working in an ever-changing environment. This is critical not only for developing and delivering top-notch mobile applications but also for ensuring the security of these applications and the data that are created, shared, and stored on and off the corporate network. Modern tools and processes are crucial for protecting invaluable enterprise data in a time when many employees carry two or more devices—a ratio that appears sure to rise as our definition of "device" expands—and as fewer and fewer people draw clear lines between the technology they use at work and at home. In this white paper, we'll examine both the challenges widespread mobility poses to businesses and strategies for unlocking mobility's potential while mitigating its risks.

## Key Points

- Mobility is everywhere—and yet it's still just beginning.
- Get ready for the Internet of Things and wearables.
- The rapid growth of data presents both immense opportunities and immense risks.
- Security is paramount for the modern, mobile business.
- The DevOps movement can help IT better meet the demands of the mobile era.

# EVERY BUSINESS IS A MOBILE BUSINESS

## The Proliferation of Mobile Devices and Applications

Consider the widespread, powerful effects mobility has had in a relatively short span of time. Technical support teams, for example, report that 15 percent of all help desk tickets are related to mobile device usage. That's an especially substantial figure when you consider that the iPhone only recently celebrated its seventh birthday.

Mobility has become a disruptive force throughout the business world. HDI noted a substantial bump in service desk tickets from 2012 to 2013, when two-thirds of survey respondents said they'd experienced a year-over-year rise in support requests. When asked to attribute the causes of the increase, mobility was an unmistakable theme among responses: the number of supported devices (31%), support for the mobile workforce (24%), and the number of supported personal devices (21%), along with overall growth in the number of customers these organizations support.

While the notion that "mobility makes things easier" might be true in certain instances, additional research found that 40 percent of technical support organizations were struggling to keep up with the rapid emergence of new mobile technologies. Another six percent said they simply weren't supporting mobile devices.

While HDI's data show that the picture has improved over the past several years—for example, more than half of support teams said they were keeping pace with emerging mobile devices—it's clear that many businesses are still playing catch-up. "When organizations can't keep up with the pace of devices rolling out to the mobile workforce, it's difficult to proactively support them," the report notes. Indeed, the survey found that while a growing number of organizations (44%) have well-defined policies for supporting mobile devices, almost as many (43%) are still developing their strategy, and 11 percent have no policy in place at all.

The report concludes on a positive note: "Organizations are shifting away from hasty support for specific devices to strategies that proactively address the needs and expectations brought about by the mobile device boom and the consumerization of IT."

And what about all of the apps running on these devices? There are a lot of them, to put it mildly: there are more than 1.3 million **Android apps** alone in the Google Play store, and a similar number in **Apple's App Store**. The latter opened in June 2008; in the six years since, more than **75 million apps** have been downloaded. An entire industry has sprung up around the development and support of so many apps across so many devices: "the app economy."

It is indeed an economy unto itself, one that, in turn, fuels the broader economic engine around it. Last year, **Gartner predicted** that by 2017 mobile users will have downloaded 268 billion apps, to the tune of $77 billion in revenue. A new study conducted by a consultancy on Apple's behalf recently concluded that Apple's mobile ecosystem has created **629,000 jobs** in Europe alone.

The changes brought about by such massive growth in a relatively short period of time are magnified when you realize that the mobile device landscape—if not the meaning of "mobile device" itself—is preparing to expand and change (again), as will the applications and data moving across those devices and the networks they connect with. The aforementioned shift in support strategies is one that has—or should have—corollaries in application development, infrastructure and operations, security, and elsewhere in the organization.

# EVERY BUSINESS IS A MOBILE BUSINESS

A recent InformationWeek survey on "next-generation IT" found that 79 percent of respondents develop mobile apps for internal customers. Yet, a follow-up question on development environments revealed that the overwhelming favorite was Windows apps, which has historically meant desktop applications. The survey revealed fragmented development across mobile platforms. "So, for all the talk of a 'mobile-first' development mindset, companies aren't quite there yet—particularly for internal users," the report concludes.

No doubt, while there are certainly early leaders with real mobile success stories, much of the business world is still sorting out the best strategies for not just managing mobility, but maximizing it.

That's perhaps one of the most remarkable things about the explosive growth of mobility in recent years: for all of its impact to date, it really is still in its early stages, with plenty of change to come. Later this year, for example, we'll see the release of Apple's iOS 8, as well the probable launch of iPhone 6 in a similar timeframe. Google's Android continues to earn massive market share, and its Chrome OS adds another subcategory to the traditional laptop market. Android is also finding its way onto more laptop models. We've already seen the hardware lines blur between phones, tablets, "phablets," laptops, and other form factors, evident in the likes of Microsoft's Surface Pro 3 and other hybrid hardware. It's safe to assume there will be similar innovations in the months and years to come. In fact, we're about to witness a whole new class of connected devices that will continue to change how we live and work.

## The Approaching Surge of the IoT and Wearables

The Internet of Things—where everything from household appliances to cars might be connected and communicating online—and wearable technologies, such as health and fitness sensors or the nascent Google Glass, aren't really new. But for most people, these trends have been more fodder for discussion and headlines than an everyday reality. Expect that to change quite soon: IDC recently projected that the market for IoT technologies will hit $7.1 trillion in 2020. Gartner estimated that the IoT will include 26 billion connected devices by the same year. These are not the numbers of niche technologies or passing fads.

As we approach that kind of growth, the IoT, as well as a corresponding rise in wearables, such as smartwatches and health monitors, will undoubtedly impact the workplace. This is not dissimilar to the way smartphones and tablets began appearing in offices everywhere, even when companies themselves weren't purchasing them for on-the-job use. However, IT departments may not be doing enough to prepare for the onslaught of new devices, application requirements, data, security issues, support concerns, and other effects of the mainstream IoT and wearables.

In a recent Spiceworks survey of IT pros, 71 percent agreed that the IoT will impact both consumers and the workplace. Yet, 59 percent say their organizations are doing nothing tangible to prepare for it.

There are considerable business opportunities associated with these two interrelated trends. There are also considerable pitfalls for organizations that don't plan accordingly for new application requests and changes to existing applications, not to mention a host of data-related issues, such as networking, security, storage, analytics, and more. Then, consider the support implications. Organizations that are just now sorting out their strategies for BYOD paradigm, for instance, will soon face an even greater challenge as the "D" in BYOD becomes synonymous with far more than phones and tablets.

In fact, 61 percent of respondents to the Spiceworks survey said they believe the number of devices per employee they'll be required to support will continue to increase over the next five years, thanks largely to the IoT and wearables. Today, roughly 70 percent say they already support two or more devices per staff member.

# EVERY BUSINESS IS A MOBILE BUSINESS

You might recall a lesson learned from the BYOD groundswell: employees don't want to hear "no" when they ask for access to business apps and data on their personal devices. (C-level executives *definitely* don't want to hear "no.") Unfettered access is rarely a good idea, and there are apps and data you'll want to restrict or prohibit altogether (for security, productivity, or other reasons), but a sound usage policy—whether the devices are company-purchased, employee-owned, or a mix of both—is an important part of a strong mobile strategy. Strategic IT organizations increasingly strive to be enablers rather than naysayers, especially given the new business arenas that mobility and related technologies facilitate. Bear in mind, enablement means more than just saying "yes" to new requests. It requires rapid, regular application delivery, the infrastructure to support growing devices, applications, and data, and the proper tools and processes to provide elite security.

## The Inevitable and Exponential Increases in Data

Just as the very definition of mobility will continue to expand and evolve, so too will the data these mobile devices and applications generate. Enterprise data growth is already pointing skyward; InformationWeek's **2014 State of the Data Center Report** found that 73 percent of IT respondents expect demand for data center resources to increase this year compared with last year. Mobile data alone will grow **6.3 times** from its 2013 level by the year 2018, according to Analysys Mason.

The **"digital universe"**—the boundaries of which are defined by all of the data generated by people and machines worldwide—will double in size approximately every two years between now and 2020, according to IDC, when we'll hit around 40,000 total *exabytes*. If the prediction comes true, that's around 5,200 GB *per person* worldwide. For some comparative context, an individual today gets between 2 GB and 15 GB in a free account with any of a number of popular cloud storage services (Dropbox, Microsoft OneDrive, Google Drive, etc.). The various iPad models range from 16 GB to 128 GB in storage capacity. A laptop with an ample 1 TB internal drive can still store "only" a maximum of 1000 GB.

Regardless of whether such industry projections hit the mark or not, you'll be hard-pressed to find anyone who thinks enterprise data needs are going to *shrink* over time. An entire industry has sprung up around Big Data, and it's not going away anytime soon. As more and more machines come online in the coming years, they'll certainly drive exponential data growth.

This kind hyperexpansion of data presents mind-boggling opportunities for productivity, analytics, and other areas. It also comes with tremendous implications for IT infrastructure, data governance, service stability and downtime, online privacy, and other areas. One area in particular should be top of mind for just about any organization as information becomes increasingly valuable: security.

## Data Security Is Everyone's Problem

For strategic organizations, mobile devices themselves are just a small part of the mobile security story. The applications that make these devices so powerful must also be secured. So, too, must we secure the data traveling between mobile devices and corporate, home, and public networks, cloud services, other computers, and so forth. Data breaches and other security events are serious business, and no one is **immune** from the consequences these days. Security awareness and training, backed by strong security technologies and IT processes, need to be part of any mobile business—which is to say, they need to be a part of *every* business.

# EVERY BUSINESS IS A MOBILE BUSINESS

Consider the BYOD phenomenon, a major reason why every business is a mobile business, whether it believes itself to be or not. Employees have been driving technological change in their organizations, something that's almost certain to continue as the IoT and wearables become commonplace.

Around one-third of respondents to a recent HDI survey indicated that their companies have formal BYOD programs in place for at least a portion of their employees and their personal smartphones, with 11 percent reporting their policy covers the entire staff. And around one in three have formal policies in place for some employee-owned tablets, with six percent of tablet policies governing all tablets.

Now, consider these projections: **Gartner predicts** that by 2017 half of all employers will *require* employees to supply their own mobile device for business use. Gartner expects a corresponding 38 percent of companies to stop providing devices to employees, according to its worldwide survey of CIOs. In that scenario, BYOD becomes not just supported but *mandated* by companies. Yet this movement comes with a clear downside: "BYOD does increase risks and changes expectations for CIOs," Gartner notes. "Unsurprisingly, security is the top concern for BYOD. The risk of data leakage on mobile platforms is particularly acute."

Whether you're in the BYOD camp or straddling both worlds, mobile businesses must consider how they'll unlock the potential of so many devices, applications, and data while minimizing the serious risks that accompany the upside.

Consider some of the findings from InformationWeek's **2014 Mobile Security Report** to get a sense of where organizations stand today:

- Half of companies allow employees to use corporate-owned devices on social networks and corresponding mobile apps. Thirty-one percent enable them for certain departments; only 19 percent ban access altogether.
- Some 40 percent express concerns about employees moving company information to cloud-based services.
- Technology defenses are a particular weak spot: just 27 percent of the government agencies included in the survey say they're currently able to prevent data from leaving employee devices.

Indeed, technology approaches play a major role—alongside policy, process, training, and other means—in sound mobile security strategy, one that looks to secure not only the device itself but also the applications it runs and the data it creates and accesses. Modern mobile security requires a holistic approach. Legacy approaches to endpoint security won't suffice.

Think in terms of tools like identity-centric management, tiered authorization and access to enterprise systems and data, multifactor authentication, monitoring and analytics, and the ability to deploy both internal and public apps via a centrally managed enterprise app store. Such technologies will play an increasingly important role in security strategies as the menu of potential devices and applications grows longer and longer over time, due in no small part to the IoT and the adoption of wearable devices. This will be underscored by commonplace BYOD implementations in the enterprise.

While many companies are thinking along these lines, it's early days yet: one in five organizations included in InformationWeek's 2014 Mobile Security Report still allow corporate data to be stored on personal mobile devices. On the other side of the spectrum, nearly half (47%) ban it altogether. There's a middle ground for BYOD organizations: one-third of organizations allow corporate data to be stored on personal devices, but only within containerized apps.

Mobile security priorities among the survey's respondents both positively signal awareness of the issues and underscore the need for robust security technology. When asked to rate certain concerns on a scale of one (not important) to five (very important), these topped the list:

- Securing company data residing on mobile devices (4.6)
- Securing devices themselves using antivirus or antimalware, MDM client software, etc. (4.2)
- Securing data in transit from the network to mobile devices (4.1)
- Keeping corporate data separate from personal data (4.0)
- Compliance, audit, and asset management (3.9)

Mobile business requires changes not only to technology tools but also to how IT teams deliver and support enterprise applications across a diverse set of devices, operating systems, and users.

## How the DevOps Approach Can Help

Longtime IT professionals are all too familiar with the slow, sometimes painful project lifecycles of the past: separate teams responsible for seemingly every function, from product to development to testing to security to support, each stamping "done" on their piece of the project and handing it off to the next team in lockstep fashion.

That approach is ill-suited for the mobile era, which demands faster, more frequent development cycles without sacrificing stability or security. Business needs change rapidly, applications require regular updates, and data must be constantly managed and analyzed. As the IoT and wearable technologies move into the mainstream, speed and flexibility will become that much more important, as will the security of new devices, applications, networks, and the constant flow of data between them. Trying to manage this—much less deliver bottom-line business value—within the constraints of old technology project processes and timelines will be akin to jamming the proverbial square peg in a round hole.

As a result, a **growing number** of organizations are embracing the speed and agility of the DevOps approach, which more tightly aligns development teams—in particular those working with the **Agile methodology**—with IT operations personnel responsible for testing, infrastructure, security, systems stability, and other pre- and postlaunch responsibilities. In essence, DevOps is a mix of technology, people, and process intended to increase IT speed and efficiency without sacrificing quality, reliability, or security (in fact, the opposite is the intended outcome).

InformationWeek's **2014 DevOps Report** found that 21 percent of respondents had already implemented DevOps in their organizations, with another 21 percent reporting clear plans to do so in the near future. That's indicative of both the growth of the movement and also the tremendous opportunities and benefits for organizations that have yet to give DevOps serious consideration. These opportunities and benefits include:

- **Faster deployments:** Forty-one percent of respondents saw "significant improvement" in the speed of their application deployments as a result of implementing DevOps, with another 42 percent reporting "some improvement." Just five percent, meanwhile, indicated they saw no improvement at all.
- **Improved stability:** Thirty-one percent said DevOps led to "significant improvement" in the stability of their IT infrastructures, with another 51 percent reporting "some improvement." Just three percent achieved no stability improvements as a result of implementing DevOps.

- **Better monitoring:** The second most common driver for DevOps adoption, at 42%, is the need to "improve our ability to monitor, alert, and audit changes to production [systems]."
- **Tighter alignment with security:** By more closely integrating security testing and sign-off with the development process, DevOps teams say they expect somewhat improved application security (35%) or significantly improved application security (10%), with 32 percent saying it will have no impact. Around seven percent expect weaker application security.

This latter potential benefit, in particular, is also a good example of how getting buy-in for DevOps is not always a straightforward task. In a sense, it's a job for security pros who have the expertise to be suspicious and point out potential problems. Similarly, other stakeholders may also have concerns—but those concerns can be turned into catalysts for change.

There's no DevOps magic wand, though. Like most significant changes to how an organization gets things done, implementing DevOps—whether as a formal department or simply as a work discipline—requires smart planning and often some corporate diplomacy. Common organizational objections to DevOps should sound familiar to IT veterans: lack of resources, lack of expertise, other business objectives and/or technology projects taking priority, a lack of demand or understanding from the rest of the organization, and so on.

Consider the following recommendations for overcoming organizational resistance:

- **Prove the business value:** Show, rather than tell, the bottom-line benefits of DevOps using advanced metrics that make sense for your organization and industry. **Sell the results**, not the hype or the "feel-good" evidence.
- **Appeal to pain points:** Identify the cumbersome headaches of people and teams that object to DevOps and consider how the approach might alleviate their pain. Take this example from the InformationWeek's **2014 DevOps Report**: "Appeal to IT staffers' dislike of audits, compliance documentation drills, and wasteful meetings...When the DevOps approach is implemented properly, many of these 'documentation' events become simple exchanges of data instead of long meetings and explanations."
- **Break down barriers, open up communication:** Clear, honest communication underpins much of the DevOps approach. In can also be one of the best tools for achieving interdepartmental buy-in. The aforementioned **DevOps report** notes that security teams are ready for the approach—and can benefit from it—but might be mistrustful. Don't pitch automation or other technology changes. "Instead, to sell the security team on DevOps, let staff sit in on the deep technical discussions that team members must have to develop the associated architecture models," the report reads. "Those discussions are pure gold for spotting security risks."

## Conclusions

Mobility will continue to create new expectations for how organizations interact not only with external customers but with employees as well. It also generates massive potential for products and services, productivity and collaboration, data analytics and insights, and more. As with most revolutionary changes, however, those opportunities aren't risk-free. Businesses will need to leverage current technologies and methodologies to not only capitalize on the benefits but also proactively manage the risks that accompany them, especially in the mobile security arena. The good news is that many organizations are moving in the right direction. But there's still plenty to be done—and plenty of change on the horizon as the scope of mobility evolves well beyond smartphones and tablets to the outer limits of our technology imagination.

## About the Author

Kevin Casey covers a variety of technology topics for InformationWeek, where he's recently been focusing on Big Data as well as IT careers and hiring trends. He also writes regularly about security, mobility, and other areas for a variety of outlets. Kevin won a 2014 Azbee Award from the American Society of Business Publication Editors for his feature story "Are You Too Old For IT?" and was a 2013 Community Choice honoree in the Small Business Influencer Awards. You can find him on Twitter **@kevinrcasey**.

## About HDI

HDI is the professional association and certification body for the technical service and support industry. Facilitating collaboration and networking, HDI hosts acclaimed conferences and events, produces renowned publications and research, and certifies and trains thousands of professionals each year. HDI also connects solution providers with practitioners through industry partnerships and marketing services.

Guided by an international panel of industry experts and practitioners, HDI is the premier resource for best practices and emerging trends.

## About CA Technologies

Mobility is changing the world. CA Technologies is changing the way enterprises manage mobility.

CA Management Cloud for Mobility powers innovation, drives productivity, and accelerates the development of new mobile applications and offerings. The capabilities offered by the industry's only Smart Containerization™ technology deliver automation that drives simplicity while effectively securing the mobile environment.

The CA Management Cloud for Mobility portfolio consists of three complementary solution suites: **Enterprise Mobility Management**, **Mobile DevOps**, and the **Enterprise Internet of Things**.

Visit us at **www.ca.com/mobility** to learn more.