

Overcome Security And Identity Management Challenges In Enterprise Mobility With The Right IT Infrastructure

Table Of Contents

Executive Summary	1
Your Workforce Will Be Empowered By Mobile Moments	2
IT Infrastructure Is Ill-Equipped To Support Enterprise Mobility.....	3
Prioritize Capabilities To Support Mobility	5
Key Recommendations	7
Appendix A: Methodology	8
Appendix B: Supplemental Material	8
Appendix C: Endnotes.....	8

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

© 2014, Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. For additional information, go to www.forrester.com. [1-RQHK0J]

Executive Summary

“Mobile moments” — when employees access immediate, contextually relevant insights from a mobile device — are poised to redefine how people conduct business. Customers will expect your employees to have a wealth of contextually relevant data at their fingertips along all steps of the customer journey, while the cost-savings opportunities of managing back-end systems with the insights from mobile devices will be paramount to maintaining a reliable ecosystem. These interactions will unlock opportunities for revenue and competitive differentiation, but companies face many challenges on the road to achieving these benefits. First and foremost, the mobile-empowered enterprise requires a suitable IT infrastructure to support it, and currently there are few legacy systems equipped to the task.

In August 2014, Microsoft commissioned Forrester Consulting to evaluate the most pressing challenges facing IT organizations for enterprise mobility initiatives. To explore these obstacles, Forrester developed a hypothesis to test the assertion that IT organizations need to build the right infrastructure to support a robust, integrated mobile ecosystem.

Enterprise mobility will drive the next generation of customer experience, employee productivity, and back-end efficiency.

In conducting an in-depth survey of 200 North American and European IT decision-makers with responsibility for mobility strategy or initiatives at companies of 250 employees or more, Forrester found that while business groups are excited about the possibilities of a mobile workforce, IT is still assessing the mountain it will need to climb to get there. The expected benefits of a well-executed enterprise mobile strategy are only outweighed by the risks of a poorly executed one. Pain points such as security, identity management, integration, and cost need to be addressed before a mobile ecosystem can thrive. If left unresolved, these issues can lead to serious repercussions in revenue and brand credibility.

KEY FINDINGS

Forrester’s study yielded three key findings:

- › **Enterprise support teams are seeing both the potential and the risk in integrating mobile across the enterprise.** While the potential is there for mobile to enable improved employee productivity and enhanced client relationships, IT professionals face a greater challenge to keep security, identity management, overall complexity, and their own costs under control. The balancing act for IT organizations is only getting harder with the shift to mobile.
- › **Security is the biggest concern for mobile support professionals.** As a part of this study, Forrester Consulting asked respondents to cite their top challenges in planning or deploying mobility initiatives. In choosing from a list of 24 challenges, respondents put security in the top six responses. Protecting the enterprise from intrusion via an exploding number of devices, applications, and data points is clearly top of mind for many IT professionals. Adding to these concerns is the tradeoff between security and user experience. Specifically, as IT professionals implement increasingly rigorous security measures, users may be turned off by the added effort to access their accounts, files, and data.
- › **Tomorrow’s mobile-ready IT infrastructure requires investment today.** The onus is on IT to transform the infrastructure to support a mobile ecosystem. No IT organization will be able to snap its fingers three years from now and be instantaneously mobile-ready; it takes a long-term strategy and continued investments. Without the right people, tools, and technology in place, your organization will not be able to meet future expectations of a mobile-empowered workforce.

Your Workforce Will Be Empowered By Mobile Moments

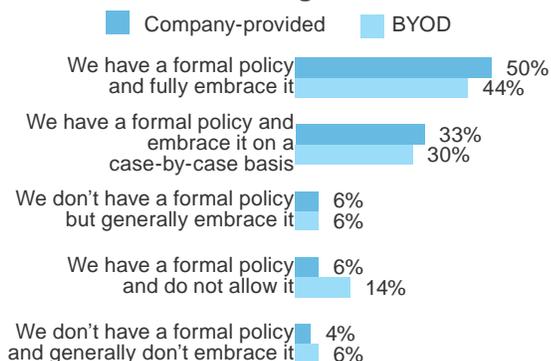
Enterprise mobility will drive businesses into the next generation of customer experience, workforce productivity, and back-end infrastructure efficiency. Once a robust mobile ecosystem is established, your employees will deliver immediate, contextually relevant “mobile moments” along all touch points of the customer journey, while mobile-empowered dashboards and analytics will allow your business to run more efficiently and mitigate risks quicker than ever before.

Until recently, enterprises have shown much interest but little tangible investment in mobility initiatives. The tides may be shifting; there are several indicators that businesses are readying themselves for full-scale commitment to executing a mobile strategy.

In September 2014, Forrester Consulting conducted a survey of 200 North American and European IT decision-makers with responsibility for mobility strategy or initiatives. The results show that 50% of organizations are beginning to make investments in monitoring and management capabilities specific to mobile. Likewise, respondents indicated that their organizations are preparing to govern this new mobile ecosystem, with 50% having a formal policy that fully embraces company-provided/subsidized mobile devices and 44% embracing bring-your-own-device (BYOD) (see Figure 1).

FIGURE 1
Companies Are Preparing To Govern A Mobile Ecosystem

“What is your company/organization’s policy on the following devices?”



Base: 200 IT decision-makers responsible for mobility strategy or initiatives

Note: Percentages may not total 100 because of rounding.

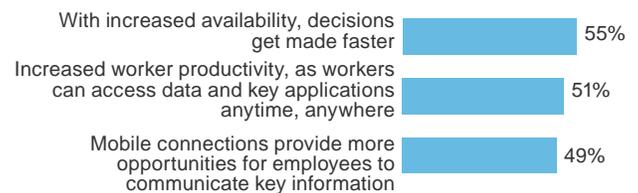
Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, October 2014

The benefits of this shift will be realized on the bottom line. Respondents indicated that investing in enterprise mobility would open up opportunities for both cost savings and revenue generation (see Figure 2). Benefits include:

FIGURE 2
Companies With Enterprise Mobility Will Enjoy Cost-Savings And Revenue-Earning Opportunities

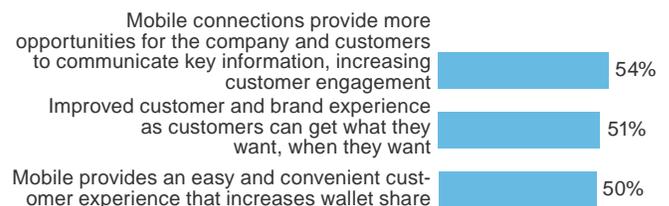
“What do you think are the biggest cost savings achieved by investing in enterprise mobility?”

(Select all that apply)



“What do you think are the biggest revenue opportunities achieved by investing in enterprise mobility?”

(Select all that apply)



Base: 200 IT decision-makers responsible for mobility strategy or initiatives

Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, October 2014

- Improved worker productivity.** IT decision-makers recognize that investing in enterprise mobility will empower workers. Fifty-five percent of respondents indicated that increased availability will open up employees to make decisions faster, and 51% anticipate worker productivity to increase as data and applications are available any place, anytime.
- Enhanced client relationships.** Enterprise mobility initiatives will enrich businesses’ relationships with their customers, leading to increased revenue. Specifically, 54% of IT decision-makers predict mobile connections will provide more opportunities for the company and customers to communicate key information, increasing customer engagement. Fifty-one percent expect improved customer and brand experience as customers can get what they want, when they want.

IT Infrastructure Is Ill-Equipped To Support Enterprise Mobility

Despite the high expectations and policies to govern mobile usage, few enterprises have dedicated substantial resources into executing their mobile strategy. Only 14% of IT decision-makers reported that their organizations have a fully robust and integrated ecosystem, supported and funded across the enterprise. Business groups may be focused on the end state of a mobile-empowered workforce, but the pressure is on IT to build the vehicle to get them there, and the current infrastructure is ill-equipped to tackle the task.

For 30 years, companies have been building the technology systems to power PCs on employees' desks and then websites on customers' PCs. They built software to connect these tools to the big corporate systems of record that manage things like inventory and customer records. The result of all this activity, in most large companies, is a technological chaos of complexity, redundancy, and antiquity. The technology they invested in to power PCs and the Web won't stretch to handle mobile moments, so they will need a new technology approach, one designed for the mobile world.¹

The enormity of the task has led to trepidation among IT decision-makers and delays to full-scale implementation of a robust, integrated mobile ecosystem. When asked if mobility initiatives would make IT operations easier, more difficult, or neither, over the next 12 to 24 months, respondents answered for every response option that IT operations would become more difficult.

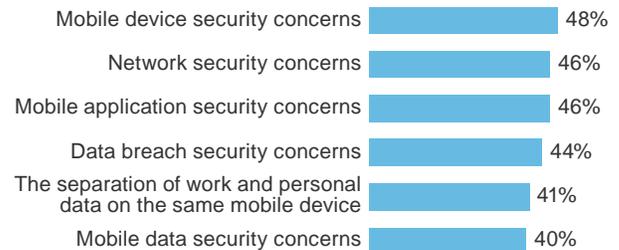
MOBILE SECURITY CONCERNS ARE KEEPING IT PROFESSIONALS UP AT NIGHT

When respondents were asked which challenges are paramount as their organization plans and/or deploys its mobility initiatives, five of the six top responses all involved security (arguably six of six, when considering "separation of work and personal data on the same device" as a security issue; see Figure 3). Likewise, maintaining a secure environment is ranked as the No. 1 biggest challenge with supporting an environment for mobility initiatives.

FIGURE 3
Maintaining Security Is The Top Challenge Facing Organizations Deploying A Mobile Strategy

"Which challenges or barriers does your organization face as it plans and/or deploys its mobility initiatives?"

(Select all that apply)



Base: 200 IT decision-makers with responsibility for mobility strategy or initiatives

Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, October 2014

The IT ecosystem has been decentralizing for decades, but many of the solutions developed along the way to maintain security aren't sufficient to cover a robust mobile ecosystem. Adding to the challenge is that security is often at odds with usability: If rigorous security measures are put in place, employees may choose to use their own unsanctioned, unsecure solutions. This presents a worst-case scenario for companies, as adoption rates for company-approved devices drop and the risk of breaches remains high. Many IT organizations are still figuring out how to balance security with usability, leading to delays in implementing the mobile strategy.

The dangers of launching an enterprise-level mobile ecosystem without addressing exploitable holes in your security cannot be overstated. According to respondents whose organizations have experienced data loss or security breaches as a result of use of mobile devices or employee-acquired devices, the consequences include:

- › **Significant expenses to troubleshoot, repair, and prevent future breaches.** The aftermath of a security breach can be expensive, as the IT organization scrambles to patch the leak and prevent future instances. Forty-two percent of respondents claim to have experienced this.
- › **A serious hit to brand credibility.** Hackers are an IT professional's worst nightmare, and not just because of

the system damage or disrupted service. The bad PR from a security breach, especially one involving customers' credit card information, can be incredibly harmful to the trust customers place in the enterprise and its systems. Forty-two percent of respondents reported that their brand suffered as a result of a breach; this was tied with the expense of a breach as a top impact.

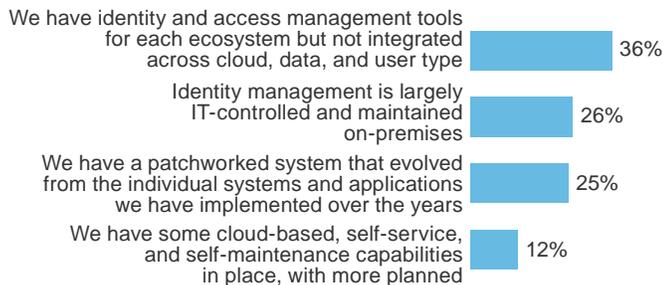
IDENTITY MANAGEMENT CHALLENGES

For today's digital businesses, identity and access management involves far more than just provisioning employees with corporate resources and enforcing the appropriate access.² Employees expect a seamless experience: This means passwords update across accounts and applications, data is available in multiple applications, file access is consistent, and, of course, none of these capabilities are limited when switching between devices. The challenge for IT organizations is that a seamless experience requires integrated identity management across back-end infrastructure and applications, and very few organizations are able to deliver this.

Thirty-six percent of IT decision-makers said their organizations have identity and access management tools for each ecosystem, but they are not integrated across cloud, data, and user type (see Figure 4). Only 18%

FIGURE 4
Identity Management Is Largely Nonintegrated Across Cloud And On-Premises

“How does your organization monitor and manage identity management across its technology ecosystem?”



Base: 200 IT decision-makers responsible for mobility strategy or initiatives
 Note: Percentages may not total 100 because of rounding.
 Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, October 2014

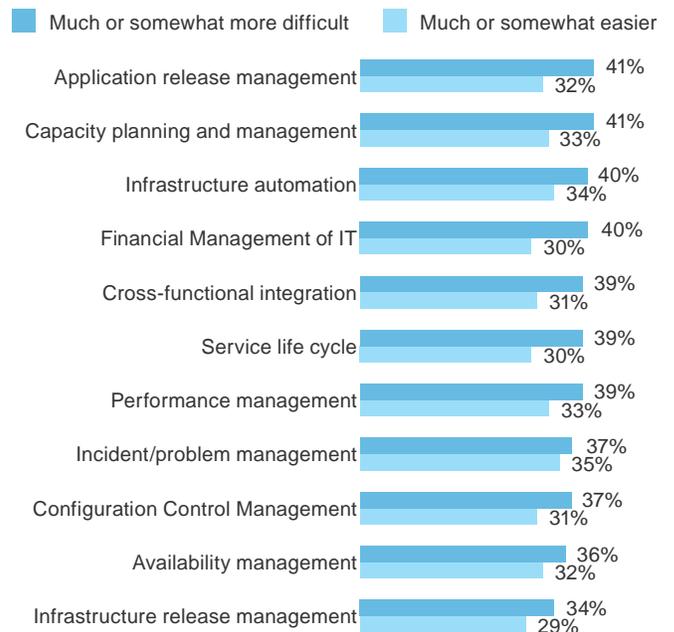
reported having an identity management system that integrates with other management systems.

MANAGING COMPLEXITY AND COSTS

Simple additions to a company's device ecosystem add significant complexity and cost to an IT organization, and mobile is much more than simple; it is a game changer. Users now need to be able to sign into the system from multiple devices in any location, any time of day. Will they see a consistent environment from every device? Will the system remain secure? What about integration and application management? Across the board, IT decision-makers believe their mobile initiatives will make IT operations more difficult over the next 12 to 24 months, outnumbering those who thought IT operations would be easier in every category (see Figure 5).

FIGURE 5
Mobility Initiatives Will Challenge IT Operations

“Rate how you think mobility initiatives will impact the following IT operations over the next 12 to 24 months.”



Base: 200 IT decision-makers responsible for mobility strategy or initiatives
 Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, October 2014

Prioritize Capabilities To Support Mobility

The reconstruction of your IT infrastructure to support an integrated, secure mobile ecosystem will be a multiyear project involving massive investments from across the organization. It will affect how your company interacts within itself and externally with customers. The potential benefits of a successful mobility ecosystem are matched by the risks of a poorly executed one, so executing the right initiatives and targeting the right technologies to upgrade will be critically important. Look to prioritize the following capabilities:

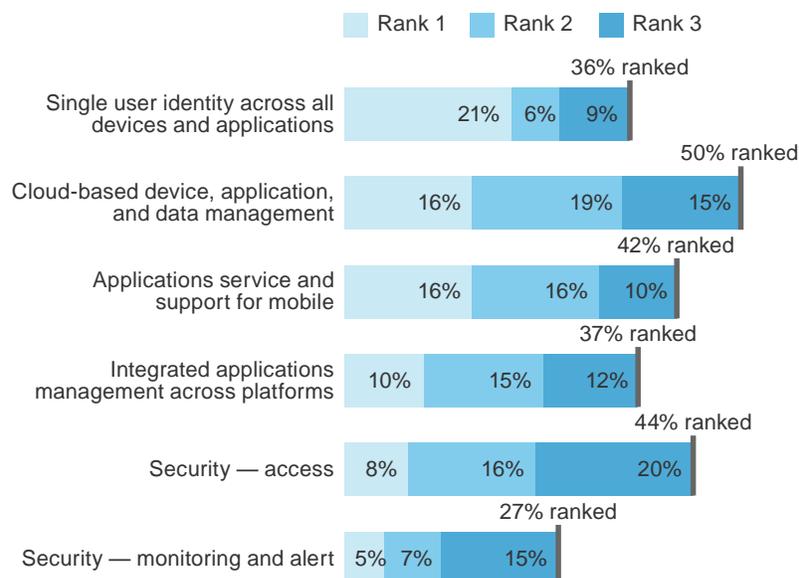
› **Single user identity across all devices and applications.** When asked what capabilities would be most important for their IT team over the next 12 months to support a mobile ecosystem, respondents ranked single user identity as the most critical (see Figure 6). Currently, business applications are equally likely to be on-premises, provided by a software-as-a-service (SaaS) vendor, or hosted by a business-to-business (B2B) partner. Letting internal app developers and SaaS apps create entirely disconnected accounts guarantees

cumbersome identity provisioning and accessing.³ Many enterprises utilize a single sign-on (SSO) service for security and identity management across cloud and non-web applications on their desktops. Extending and integrating this with mobile devices will lead to the end user benefits of faster and easier login, as well as simplified password resets and synchronization. SSO sets the stage for balancing a beneficial tradeoff between security and usability.

› **Access security.** While only 8% of IT decision-makers surveyed ranked access security as their top concern, it is still considered a priority. Forty-four percent of IT decision-makers ranked it among their top three most important capabilities for IT teams building support infrastructure for a mobile ecosystem. As the ecosystem becomes more complicated, identity-level security is increasingly just the baseline level of security your enterprise will need. Access security is no longer just about privileging at the user level; it must also address the application, file, and data levels.

FIGURE 6
IT Organizations Will Need To Evolve Their Capabilities To Support Mobility

“What are the three most important capabilities that you think your IT team will need in the next 12 months to most successfully integrate and support mobile applications?”



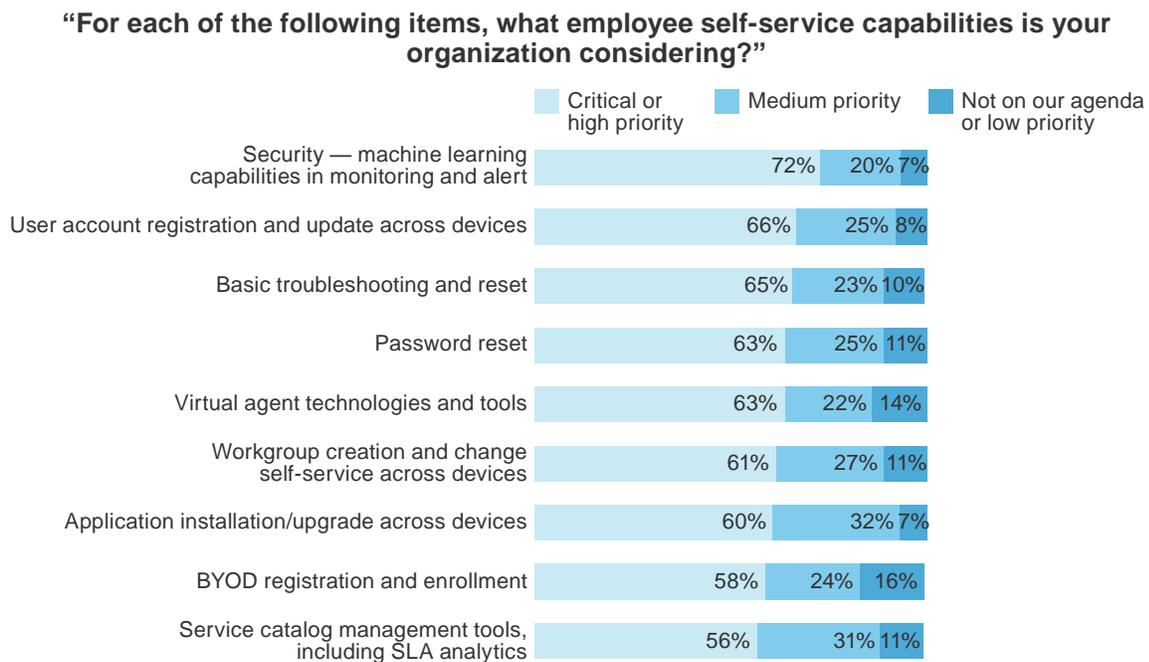
Base: 200 IT decision-makers with responsibility for mobility strategy or initiatives

Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, October 2014

- › **Cloud-based device, application, and data management.** This is considered among the top three most important capabilities by 50% of the respondents surveyed. Getting devices, applications, and data up and running in the cloud will ensure your employees can work effectively anytime and anywhere they can access the Internet.
- › **Employee self-service for lower-risk security measures.** With the cost of sweeping updates to IT infrastructure likely to leave your purse strings a bit tighter, it is always important to identify opportunities for cost savings. Employee self-service in areas like password reset, basic troubleshooting, and application reset are low-risk areas to entrust employees to solve their own issues, assuming they are given the necessary tools and training to do so. Eighty-three percent of the IT respondents said their organization provides advice and guidance to employees on how to take security precautions, and three-quarters claimed they provide self-management tools to employees. Monitoring and alerting for security, which was ranked as one of the least crucial

capabilities IT will need in the next 12 months, is much better suited to be placed in the hands of the end users, as 72% of respondents said it is a critical or high priority when it comes to employee self-service capabilities (see Figure 7).

FIGURE 7
Low-Risk Capabilities Can Be Handled By Employees Themselves



Base: 200 IT decision-makers with responsibility for mobility strategy or initiatives

Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, October, 2014

Key Recommendations

In the near future, enterprises will find themselves in one of two factions for mobile: the “haves” and the “have-nots.” The haves will consist of companies that made adequate investments in mobile initiatives early on. These companies will reap the benefits of a mobile-empowered workforce, having overcome the growing pains in IT infrastructure before their competition could figure it out. The have-nots will be the late-adopters: companies that dabbled on the fringes of enterprise mobility or never dedicated the necessary resources to refigure their back-end systems to support the mobile ecosystem. The have-nots will be hard-pressed to compete with the much more agile, customer-focused mobile-enabled enterprises, and they may find themselves being pushed out of the marketplace.

Mobile haves will take the following steps to ensure a bright mobile future:

- › **Take a proactive approach to mitigating security threats.** Even with comprehensive security measures in place, companies are still at some risk for a breach. Baseline security policies on mobile devices, such as password entry, remote lock, and remote wipe, have been around for years and are not adequate to protect your ecosystem today. Consider the next level of security beyond users: Application, file, and data-level security capabilities are needed to keep your enterprise safe. Furthermore, look for security measures that protect your organization, but not at the expense of usability. It is a delicate balancing act between security and usability, so make sure your employees know why additional, and sometimes rigorous, security measures are necessary and get their feedback on how you can improve the user experience. And in the case of that dreaded security breach, ensure that your company has standard policies for patching the leak, as well as PR teams ready to defend your brand.
- › **Invest in tools and partners to help manage your device ecosystem.** When establishing and executing your mobile strategy, be clear about your strengths and weaknesses in all aspects of your ecosystem, from people to technology. Honestly evaluate the skillsets and experience levels within your IT organization and determine where the gaps are in order to complete an infrastructure transformation. Determine if the suite of tools you have in place is adequate to cover the gaps. You're in this for the long-term — make sure your people, tools, and partners are as well.
- › **Use your CIO as a champion of your strategy to gain buy-in from across business and IT groups.** Mobility initiatives cannot be a pet project or part-time responsibility. Your company must be prepared to invest the proper internal resources in enterprise mobility, and the CIO has the best strategic viewpoint, both within IT and the business, to champion this cause. He or she must work with business leaders to integrate mobile both as a technology and a business initiative.

Appendix A: Methodology

In this study, Forrester conducted an online survey of 200 IT decision-makers in North America and Europe (UK, France, and Germany) to study best practices and challenges around mobility strategies of enterprises today. Survey participants included IT managers and directors responsible for mobility strategy and who have direct influence into decisions related to strategies and road maps for mobile device management and/or end user computing in their organization.

Questions provided to the participants asked about their perception of mobile's business impact and importance, what their current mobile environment looks like, what their challenges are, and what mobile initiatives they are planning in the next 12 to 24 months. The study began in September 2014 and was completed in October 2014

Appendix B: Supplemental Material

RELATED FORRESTER RESEARCH

Ted Schadler, Josh Bernoff, and Julie Ask, *The Mobile Mind Shift: Engineer Your Business to Win in the Mobile Moment*, Groundswell Press, 2014

"Evolve Your Identity Strategy For Your Digital Business," Forrester Research, Inc., August 15, 2014

"Brokered Cloud Identity Is Scaling New Heights," Forrester Research, Inc., October 16, 2013

Appendix C: Endnotes

¹ Source: Ted Schadler, Josh Bernoff, and Julie Ask, *The Mobile Mind Shift: Engineer Your Business to Win in the Mobile Moment*, Groundswell Press, 2014.

² Source: "Evolve Your Identity Strategy For Your Digital Business," Forrester Research, Inc., August 15, 2014.

³ Source: "Brokered Cloud Identity Is Scaling New Heights," Forrester Research, Inc., October 16, 2013.