

May 2009

Understanding The Critical Role Of Device Management And Security In Your Business' Mobile Strategy

*How IT Can Provide Better Mobility Support To Its
Anytime, Anywhere Workers Despite A Proliferation Of
Increasingly Diverse Mobile Devices*

A commissioned study conducted by Forrester Consulting
on behalf of Sybase

TABLE OF CONTENTS

Executive Summary	3
Key Findings	3
Mobility Creates New Efficiencies For The Business But Also Some Challenges For IT.....	4
Firms Are Not Keeping Pace With A Twofold Challenge: Mobile Device Management And Security	6
Firms Find That Mobile Device Management And Security Solutions Are A Necessity.....	6
The Top 10 Mobile Device Management And Security Best Practices.....	9
Study Conclusions.....	11
Appendix A: Methodology	13
Appendix B: Related Research.....	15

© 2009, 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.

Executive Summary

In January 2009, Sybase commissioned Forrester Consulting to assess the importance of mobile device management and, in particular, mobile security and the associated issues that keep CXOs up at night.

While conducting in-depth interviews with 30 IT and telecom/network decision-makers at North American and Western European companies with 500 or more employees, Forrester found that these IT professionals:

- Anticipate that the number of mobile devices they support will continue to increase through 2010, despite the global economic recession.
- Recognize that mobile devices need to be managed and secured in the same way that PCs are today, although most admit that they don't do this yet.
- Are feeling increased pressure from C-level executives, line-of-business managers, and employees to support more mobile platforms and even personal mobile devices.
- Prioritize security as the No. 1 consideration when making changes to their mobility strategy.

Key Findings

Forrester's study yielded four key findings:

- Despite tightening budgets as a result of the global economic recession, 28 out of the 30 IT professionals we interviewed anticipate that the number of mobile devices they support will increase through 2010.
- Firms are increasingly embracing more than just one mobile platform, making it critical that they invest in tools that can support mobile devices powered by BlackBerry, Windows Mobile, Symbian, Mac OS X, and Windows CE.
- With the changing workforce, IT is feeling intense pressure from C-level executives, line-of-business managers, and employees to support personal devices and applications, making security a major concern.
- Companies are increasingly investing in mobile device management and security solutions that will help automate support tasks, streamline the operations of enterprise mobility, and secure the data.

Mobility Creates New Efficiencies For The Business But Also Some Challenges For IT

As businesses embrace mobility, IT professionals are facing new challenges. But gone are the days when stodgy IT departments would fight this business imperative. Most organizations today are simply trying to get smarter about how to manage and secure their increasingly mobile population and distributed assets.

Businesses searching for a competitive advantage and striving to attract talent in today's job market are embracing the mobile workstyle for a larger percentage of employees than ever before. This is creating new efficiencies and growth opportunities — but also new challenges for IT. Companies turn to mobility to: improve employee flexibility by allowing workers to be productive independent of their physical location; to enable workers to have more control over their work hours; to increase the overall speed of business; and to improve customer satisfaction with quicker response times and more informed decision-making. But IT is grappling with how to manage and secure an increasingly mobile population and infrastructure. Specifically, IT professionals tell us that:

- **Workers are becoming increasingly distributed and mobile; work is no longer confined to always-connected devices.** The need of the workforce to remain constantly connected to peers through voice, SMS/MMS, email, instant messaging (IM), and social networking technologies has given rise to the smartphone as the *de facto* tool for workers who need to be productive while on the go. First adopted by executives, they're now widely deployed to those information workers who need access to information while on the go and to those task-based workers who don't just need access but also have to create content while out in the field. The ever-evolving needs of mobile workers are extremely diverse and result in a variety of form factors, operating systems (OSes), applications, and security requirements, but there was one common theme across the firms we interviewed: The number of smartphones supported is on the rise — and this growth will remain strong, despite the global economic recession.
- **Younger and more tech-savvy employees (Millennials) have loftier mobility expectations of IT than Baby Boomers.** Millennials grew up with the Internet, are always connected with friends and family on their smartphones, and have little patience for communication delays. They're more tech-savvy than the retiring class of Baby Boomers, who were simply happy if technology worked. IT needs to cater to the loftier mobility expectations of Millennials because it's a way in which the business can differentiate itself in the workforce and can remain attractive in today's job market. One of the ways in which firms are enabling more flexibility for this emerging workforce is by providing them with greater access to laptops and smartphones.

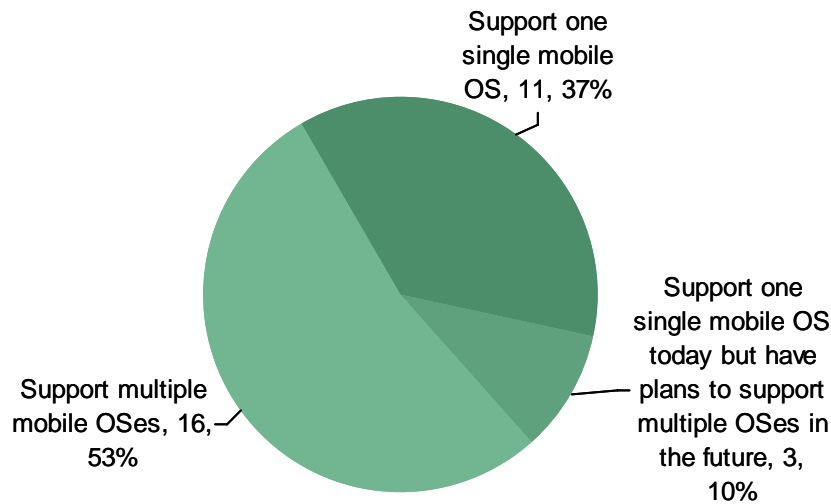
"We need to attract the right kind of talent. No one wants to go to work for a company if they're handed an old gray x86 desktop. We need to be more flexible, as we're seeing younger people coming out of college that want iPhones, laptops, etc." (Senior architect, US-based manufacturing firm)

- **They're supporting an increasing diversity of devices, OSes, and applications, and new devices often conflict with their corporate standards and sourcing practices.** The mobile landscape of today's organizations is very muddled, with different technologies, standards, and support practices; it resembles the Wild West when compared to your standardized, centrally managed, and secured PC environment. And faced with overwhelming pressure from C-level executives, line-of-business (LOB) managers, and employees to support non-standard and even consumer-grade devices and applications

(e.g., iPhone, Android, iTunes, Google Maps, etc.), IT organizations have long given up the dream of delivering the one-size-fits-all model that promised to over-serve some workers but under-serve most (see Figure 1).

“People bring in devices every day and ask for integration. It’s a personal choice thing. We want to enable that. We need to maintain the ability to attract the right kind of talent. Giving people the choice is seen as a benefit, especially for younger employees.” (Senior architect, US-based manufacturing firm)

Figure 1: More Than Half Of Firms Support Multiple OSes, And 10% Have Plans To Do So



Base: 30 senior IT managers involved in mobile device management and security in public and private organizations in the US and Western Europe

Source: US and Western European phone survey conducted by Forrester Consulting and commissioned by Sybase, February and March 2009

- **They’re facing heavy pressure to support personal and consumer devices and applications.** Not wanting to get in the way of workers being productive, half of the IT professionals we spoke with also support personal devices to a limited extent. IT traditionally requires workers to get their direct manager’s approval for access; when granted, they also require that they sign a policy document that essentially states that their personal device is now a corporate asset that’s centrally managed and secured by IT. In other words, if an employee is let go, their device will be remotely wiped and restored back to factory default conditions. Access to work resources on personal devices is often restricted to email, contacts, and calendars, but this is sufficiently alluring that IT anticipates significant growth in these pilot programs.

“With the iPhone 3G, adoption went through the roof. It was overnight. Unfortunately, a lot of people didn’t realize that they’re not going to get the seamless consumer experience. You need security, Wi-Fi, VPN, and passwords. You don’t realize how bad the experience is going to be once we lock it down.” (Lead architect, US-based financial services firm)

Firms Are Not Keeping Pace With A Twofold Challenge: Mobile Device Management And Security

Due to their small form factors, handhelds are left behind in taxis and stolen out of jacket pockets more frequently than IT would like. And while handhelds typically run fewer applications than a laptop or desktop, installing new applications or making changes to devices in the field is much more complex than on PCs. Why? Because they're not hardwired into the corporate LAN at all times, nor are they all running a standard corporate image. This lack of insight into — and control over — security, applications, usage, and the backup and recovery of handhelds has IT running ragged, especially without a central console to configure, deploy, and manage devices over the air (OTA). IT professionals cited two areas in which they need to streamline operations:

- **Mobile device management.** With more confidential and sensitive data finding its way onto smartphones, handheld devices, and removable storage cards, mobile device management solutions have quickly become a must-have solution for businesses of all sizes. And with IT facing plans for the deployment of LOB applications, burgeoning content like rich media for training purposes, and collaboration/unified communications, as well as support for more heterogeneous devices, and refreshes within the next 12 to 18 months, now is as good a time as ever to consider investing in a mobile device management solution.
- **Mobile security.** With the shift from information applications to LOB applications, increased amounts of data reside on devices and removable storage that are much more susceptible than PCs to loss and theft. And while most IT managers agree that mobile devices need to be managed and secured just as their PCs are, most don't do this today. This has driven some businesses to deploy a mobile security solution, often in addition to a management solution that doesn't have robust security capabilities.

"I think mobile device management and mobile security very much go together. Now we are evaluating the management platforms in combination with their security capabilities. Previously, we tracked mobile devices through a spreadsheet, but it was too manual and the number of devices grew too large." (Telecom manager, Denmark-based manufacturing firm)

Firms Find That Mobile Device Management And Security Solutions Are A Necessity

The key is to understand the critical role of device management and security solutions in your business' mobile strategy. By doing this, your business will be well-positioned for the next phase of mobility, which will be driven by LOB applications, mobility shifting down the corporate pyramid, and a phenomenon we call Tech Populism. When evaluating mobile device management and security solutions, consider the following key selection criteria:

- **Security policy.** When — not if — devices are lost or stolen, the data needs to stay secure. Your highest priority should be the security policies within the mobile device management solution, which include strong password enforcement, power-on passwords, authentication, multiple encryption options (e.g., the ability to use and encrypt data on removable storage cards), multiple user authentication options, and credential expiration options. And, of course, the No. 1 feature that any mobile device management point

product or suite should deliver is the ability for IT — and even, in some cases, the end user — to remotely lock and (selectively or completely) wipe a lost or stolen device.

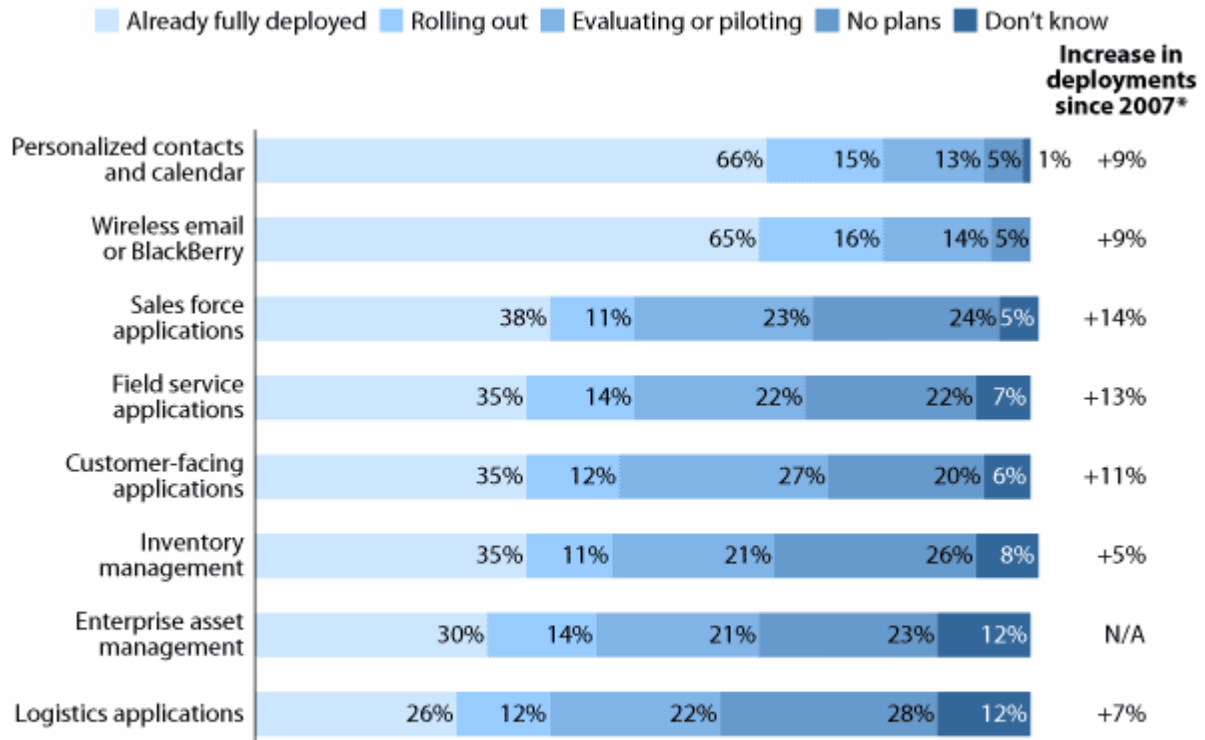
“The mobile security rules are different for our three business divisions. Each division has its own security manager. So we have three policy sets — one for each division — but these are then applied globally. The policies are reviewed whenever something significantly changes (e.g., the introduction of a new device, a new service, etc.).”
(Product manager for mobility solutions, Switzerland-based financial services firm)

- **Asset management and reporting.** Given the high rate of change and speed with which your mobile population is growing, you'll need complete insight into your current inventory of hardware and software. Asset management capabilities often come built in with software license compliance tools and inventory-based administrative alerts, which always prove useful for IT administrators who don't have the time or bandwidth to carefully monitor the console. These capabilities make completing a mobility assessment almost instantaneous and keep a log that helps with planning for future capacity.

“What we really would like to have is a consolidated device and asset management platform — even going beyond mobile devices and incorporating PCs. But, currently, we have to make do with what we have.” (Product manager of collaboration, UK-based healthcare and pharmaceutical firm)

- **Device provisioning and settings management.** IT professionals require the ability to configure a new device that comes into the field or reconfigure existing devices that go down. However, it's critical to ensure your solution has the capabilities to do it OTA so that users don't have to manually tether their device to their desktop or laptop. Most mobile device management point products or suites provide this functionality, finally making the USB cable a thing of the past.
- **Application management.** Application management capabilities are becoming increasingly important for IT decision-makers who recognize the value in mobility and think beyond wireless email and personal information management (PIM) — especially as they look to mobilize task-based workers on specialized handheld devices like those from Motorola's Symbol or Intermec (see Figure 2). As a result, in addition to configuration settings to push out to your mobile devices, IT requires remote software distribution and update capabilities. If you allow personal devices to connect to the corporate network, you'll also want the ability to whitelist and/or blacklist certain applications, like the mobile browser, IM, or video. Remember to focus on the end user experience of application deployments and test for the ability to delay or silently install applications.

Figure 2 Mobile Application Adoption Among North American And European Enterprises
"Which of the following best describes your company's adoption of each of the following mobile applications?"



Base: 243 mobile technologies and services decision-makers at North American and European enterprises (percentages may not total 100 because of rounding)

Source: Enterprise And SMB Networks And Telecommunications Survey, North America And Europe, Q1 2008

*Source: Enterprise Network And Telecommunications Survey, North America And Europe, Q1 2007

46363

Source: Forrester Research, Inc.

- Central console for remote management.** Most of today's mobile device management consoles are Web-based, which means no more thick applications to deploy. Moreover, they're compatible with most conventional browsers, such as Internet Explorer and Firefox, and support multiple administrators. The result? IT administrators can manage their mobile environments from any device they have, including their own handhelds. In other words, gone are the days when you'll have to drive to the office on a Saturday afternoon because an employee was careless with their handheld. Keep in mind that the various solutions differ significantly in appearance, ease of use, and the quantity and quality of usage reports that these consoles can generate on the fly.

"The biggest challenge regarding remote management is the sensitivity of the data that is stored on the mobile device. With the BlackBerrys, we can send out kill commands. But for the PDAs, there is not much that we can do. We are aware of the fact that our PDAs are protected less, but they only have low-level data anyway. Generally speaking, one of our major challenges is to push out suitable business applications for mobile devices. My feeling is that there are not many mature applications out there that

our business units can take advantage of yet.” (Systems and technology director, UK-based construction and engineering firm)

- **OTA intelligence, troubleshooting, and support.** Be sure to look for real-time monitoring of the health of a mobile device, logging of activities, and the ability to generate Web reports for help desk staff. Some solutions even allow administrators to remotely log in to an employee's handheld to troubleshoot it. While this functionality sounds similar to what you might be accustomed to if you've used client/desktop management tools before, these capabilities have been optimized for wireless networks. For example, make sure that: you can push out software updates with just the changes and not the entire file; you can restart the transfer in the event of an interruption or wireless dead zone; and the distribution mechanism is bandwidth-sensitive.
- **Device flexibility.** While a few mobile device management solutions excel at supporting a single operating system extremely well, the majority strive to be as open as possible. It's critical that your mobile device management solution supports multiple mobile OSes — including BlackBerry OS, Linux, Mac OS X, Palm OS, Symbian, Windows CE, and Windows Mobile — and even multiple desktop operating systems, including Linux, Mac OS X, Windows XP, and Windows Vista. These mobile and desktop operating systems cover a wide selection of devices and form factors — all the better for organizations that have been unsuccessful at standardizing their hardware or that have already embraced Tech Populism.

“Today, we support about 800 BlackBerrys, 3,000 Windows Mobile smartphones, and a few iPhones. Mostly, staff can get the mobile devices that they want. We only tell them the capabilities that the devices need to have, and then people get what they want. Depending on your position, you can expense your mobile bills. This varies by job responsibilities.” (Director of infrastructure and desktop management, US-based public-sector firm)

- **Backup and recovery.** No management platform is complete without the capabilities for automatic backup and recovery of settings, files, and applications. This is particularly important given how often devices are dropped onto concrete sidewalks or replaced due to theft or loss. Moreover, backup and recovery can help with rapid transition to new devices, a common occurrence in today's volatile device market that often sees quick refresh cycles of one to two years.

The Top 10 Mobile Device Management And Security Best Practices

Implementing a device management point product and suite is the first — and most critical — step toward solving your organization's mobile device management and security challenges. To assist organizations in determining what policies to put in place, here's a list of the top 10 mobile device management and security best practices:

- **Enable device diversity.** Task-based workers who use LOB applications in the field, often in rugged environments, are well suited for Windows Mobile-powered smartphones and PDAs, whereas information workers often demand BlackBerry, Nokia E-series powered by Symbian, or iPhone devices for personal information management applications. It's important for IT professionals to segment their mobile workforce to ensure their users are receiving the form factors, devices, applications, and levels of security that enable them to be most productive while on the go. And equally as critical is to invest in a mobile device

management solution that supports multiple platforms enterprisewide, so you're not locked into a single platform for your diverse user needs across multiple departments or lines of business.

"Today, we support mainly Symbian and Windows Mobile, but we feel that we have to open it up to other devices. When you look at the trends of collaboration and Web 2.0, we think that we cannot impose any particular kind of smartphone but have to accept any kind of mobile device. I guess there will be a lot of iPhones out there in the future. Once our management platform supports the iPhone, we will offer support to these devices as well." (Systems manager responsible for mobile, Sweden-based public-sector firm)

- **Enforce a strong password policy.** Because of mobile devices' inherent vulnerability to misplacement and theft and their always-on status, it's critical that firms protect themselves through a strong password policy. All devices should be protected through strong passwords that require a refresh after between 3 and 6 months in use. Additionally, most of the companies with which we spoke also enforce remote lock after a specific period of non-use. Interestingly, the time period ranged from as little as 3 minutes to as long as 72 hours.

"Our mobile devices are password-protected and lock automatically after a period of inactivity. People know that they have to handle the data on their mobile devices with care, and they are aware of the data protection acts." (Head of group security, UK-based construction and engineering firm)

- **Remotely lock or wipe all lost or stolen devices.** Because devices are often left behind in taxis or stolen, it's important that IT has the capability to send a remote lock or wipe command to protect the data that resides on the mobile device. In the event that a user simply misplaces their device temporarily, users feel reassured knowing that their personal data will remain protected until they find their device again and unlock it or that they can fall back on wiping it if they fail to retrieve it.
- **Automate remote device wipe after 10 unsuccessful authentication attempts.** With workers juggling dozens of passwords, it's understandable if they enter the wrong password from time to time or mistype due to the small or virtual keyboard. But after 10 repeated unsuccessful authentication attempts, mobile devices should be automatically wiped. This will prevent people with malicious intentions from cracking it through brute force measures, but it also requires users to be extra careful when entering their password after several unsuccessful attempts.
- **Encrypt the data.** Consider file-level, application-level, or full-disk encryption to secure sensitive data and provide legal safe harbor from disclosure requirements in the event of lost or stolen mobile devices or removable media cards. Also ensure that all sensitive and confidential data is encrypted when it's in transit over the air between mobile devices.

"We enforce encrypted data on all mobile devices (e.g., data is in an encrypted region like a virtual file share). We also use pretty strong password protection, and the mobile devices automatically lock after a few minutes of inactivity. Policy checks are done by the software. We have the ability to wipe any device. Once we discover that a device is lost, we wipe it out immediately." (Director of infrastructure and desktop management, US-based public-sector firm)

- **Enable support for dual-usage models.** It has quickly become a necessity for firms to allow the dual usage of mobile devices that contain both professional and personal profiles, data, and applications on a single device. Application-level or file-level security (including a strong password policy and encryption) will allow personal usage to continue without change, while allowing IT to securely manage corporate data.
- **Manage all devices but limit the data stored on unmanaged devices.** For unmanaged mobile devices, consider limiting the amount of data that resides on them. Two of the ways in which firms are succeeding are by utilizing document portals or by using Web-based applications. For example, rather than sending documents back and forth via email, users send links to documents that are stored on the portal. Not only does this decrease the mobile data usage on a month-by-month basis, but it also minimizes version-control issues as users collaborate.

“We try to limit the data that is stored on mobile devices. For instance, we use a document management portal; we encourage people to only send links to the files and not the files themselves. It is a ‘best practice’.” (Technology and infrastructure director, Italy-based media and entertainment firm)

- **Avoid the company logo and display a telephone number on the locked state.** IT professionals should remove any company logos from their mobile devices because they only encourage thieves to try to extract data from them. Additionally, when mobile devices are lost and in a locked state, the screen should display a telephone number that good Samaritans can call to report that they have found the device.
- **Utilize a single Web-based console for all management and security operations.** Rather than commuting into the office on a Saturday afternoon because a user reported that they misplaced their mobile device, use the Web-based console to send that remote lock or wipe command. In fact, some administrator consoles can even be accessed through an administrator's mobile device, so you don't even have to boot up a PC.
- **Provide multichannel training and links to additional resources.** One of the most significant concerns among IT was that they aren't made immediately aware of lost or stolen mobile devices. While it's impossible to automate employee behavior, it's critical that all users are properly trained to react to certain situations and ensure they're well versed in corporate and regulatory policies. These training sessions should be provided when employees come on board, but rolling refresher training sessions should also be provided on an as-needed basis for high-maintenance or technophobe employees.

“Timely notification of lost or stolen mobile devices is key. It's a matter of educating the users of how important it is to report these incidents immediately. The notification process is not perfect today.” (Director of IT operations, US-based financial services firm)

Study Conclusions

Forrester's in-depth interviews with 30 IT and telecom/network decision-makers at North American and European companies with 500 or more employees revealed that firms can increase employee satisfaction, improve customer service, and create revenue expansion through new investments in smartphones. To continue on this extended mobile enterprise trajectory and realize true ubiquitous mobility, businesses need to execute on three imperatives.

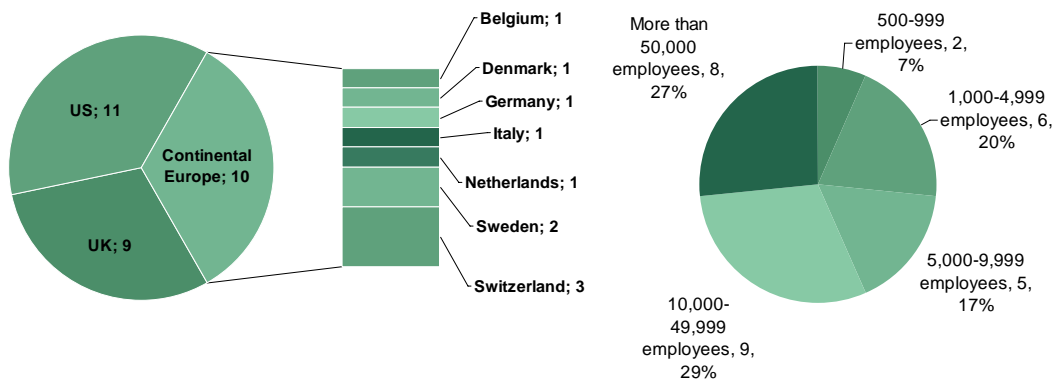
- **Manage and secure mobile devices just like PCs.** While the first phase of mobile device deployments is typically limited to wireless email, contacts, and calendars, organizations are increasingly taking it to the next level by extending access to LOB applications, such as sales force, field service, and inventory management. With increasing amounts of data finding its way to mobile devices, IT professionals need to manage and secure mobile devices just like any other endpoint on their network.
- **Get smarter about managing and securing mobile devices — now.** There are comprehensive mobile device management solutions available on the market today that can address most business and technical requirements. Alternatively, businesses can also consider outsourcing this function to a services provider. Whatever direction you choose to move in, now is the time to establish or revisit your mobility strategy. With new devices, platforms, applications, and services coming to market that promise to impact today's standards, it's critical that organizations have a plan to cope with these new technologies and services.
- **Make mobile device management and security solutions the foundation of a business' mobile strategy.** A comprehensive mobile device management and security solution should be at the heart of any business' mobile strategy. Choose which devices to support based on the capabilities of the management platform, and tailor your security requirements to the various user profiles supported. The Web-based management console should be IT's central console for all of its remote management and security needs. Investments in mobile device management solutions will have an immediate impact on the mobile operations of the business. It will lighten the support burden on IT professionals and afford them more time to work on strategic projects, not just keeping the lights on.

For an overview of vendors in the mobile device management and security market, please refer to the first document listed below in Appendix B: "Related Research."

Appendix A: Methodology

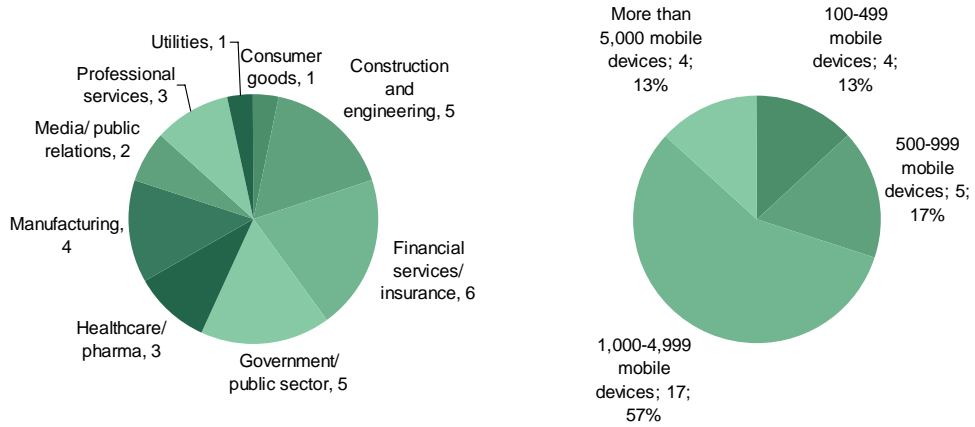
Forrester conducted a phone survey of 30 IT and telecom/network decision-makers at North American and Western European companies with 500 or more employees (see Figure 3). We interviewed both public and private organizations spread across multiple industries (see Figure 4). Eleven of the interviewees were based in the US; 10 were based in Continental Europe; and nine were based in the UK. The focus of the study was to develop an independent and objective thought-leadership paper that assessed the importance of mobile device management and mobile security and that educated the market on mobile device management and security best practices. The survey respondents were screened by geographic region, company size, and the specific functions that respondents had authority over in IT. The phone surveys were administered in February and March 2009.

Figure 3 Locations And Size Of The Interviewed Organizations



Source: US and Western European phone survey conducted by Forrester Consulting and commissioned by Sybase, February and March 2009

Figure 4 Industries And Number Of Supported Devices In The Interviewed Organizations



Source: US and Western European phone survey conducted by Forrester Consulting and commissioned by Sybase, February and March 2009

Appendix B: Related Research

[“The Forrester Wave™: Mobile Device Management Solutions, Q2 2009”](#) by Benjamin Gray, April 27, 2009.

[“Inquiry Spotlight: Mobile Device Management, Q2 2009”](#) by Benjamin Gray, April 16, 2009.

[“Building Your Business' Mobile Strategy”](#) by Benjamin Gray, April 13, 2009.

[“Enterprise Mobile User Forecast: Mobile “Wannabes” Are The Fastest-Growing Segment”](#) by Michele Pelino, October 9, 2008.

[“Inquiry Spotlight: Enterprise Mobility, Q4 2008”](#) by Benjamin Gray and Chris Silva, October 7, 2008.

[“The Mobile Operating System Wars Heat Up”](#) by Benjamin Gray, July 28, 2008.

[“Build Your Business's Mobile Strategy Around Device Management And Security”](#) by Benjamin Gray, July 22, 2008.

[“Forrester TechRadar™: Enterprise Mobility Infrastructure, Q3 2008”](#) by Chris Silva, July 14, 2008.

[“The Business Mobility Imperative”](#) by Chris Silva and Benjamin Gray, June 9, 2008.

[“Answering The Most Frequently Asked Mobile Device Management Questions”](#) by Benjamin Gray, April 18, 2008.

[“Treating Wireless Email Headaches”](#) by Michele Pelino, Benjamin Gray, and Chris Silva, April 17, 2008.

[“Forrester TechRadar™: Enterprise-Class Mobile Devices And Management Solutions, Q1 2008”](#) by Benjamin Gray, January 31, 2008.