Enterprise Strategy Group | Getting to the bigger truth.™

White Paper

Addressing Mobile Device Security and Management Requirements in the Enterprise

By Jon Oltsik

October, 2010

This ESG White Paper was commissioned by Juniper Networks and is distributed under license from ESG.

Contents

Executive Summary

In late 2009, ESG conducted a research survey of 174 IT professionals in North America. Survey respondents worked at enterprise organizations with more than 1,000 employees. Based upon this research project, this paper concludes:

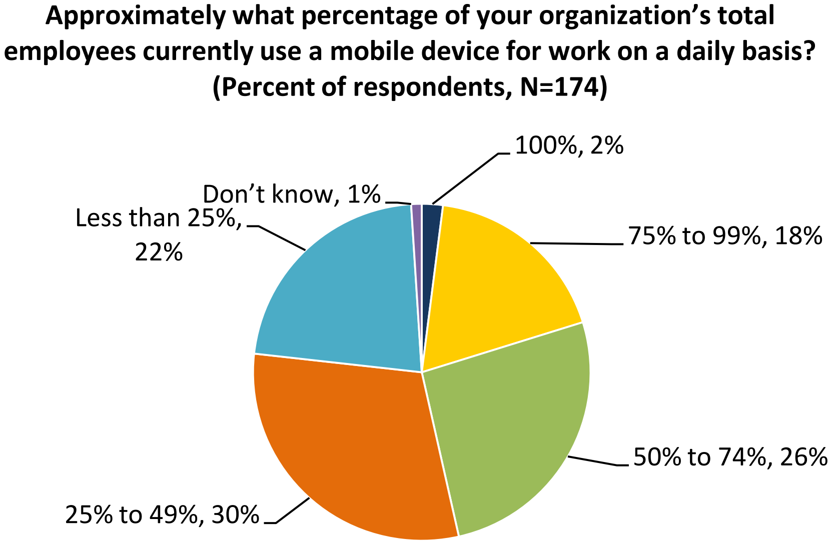
- **Mobile devices have become mission critical.** Organizations are spending more on—and doing more with—mobile devices each day. ESG's data clearly indicates that most enterprises regard mobile devices as mission critical tools, not the latest consumer toys.
- **Management and security lag behind.** Mobile devices are making employees more productive from more places. This is encouraging large organizations to invest further in mobile devices and develop custom applications. Unfortunately, the data also indicates a growing mobile device security and management gap: mobile devices tend to be managed on an ad-hoc basis, increasing IT operations cost and complexity. Alarmingly, mobile devices remain relatively insecure even though they are used to access core applications and lots of sensitive data. These issues create a potential Faustian compromise in the future as greater productivity comes with a cost of IT operations fire drills and increasing security risk.
- **CIOs must address management gaps to maximize mobile device benefits while minimizing the risks.** Large organizations need to address mobile device security and management weaknesses. What's needed? Sound policies, documented processes, integrated mobile device management and security tools, and constant oversight.

CIOs must establish a baseline of strong mobile device security as soon as possible. Why? Mobile devices represent the proverbial "weak link" in the security chain; therefore, poor mobile device security creates vulnerability for ALL critical systems on the corporate network. In other words, one compromised mobile device could lead to a major data breach. Furthermore, mobile device proliferation will only increase in the future—growing more complex, costly, and risky over time. Enterprise firms need to get their arms around mobile device security before they are buried by overwhelming cumbersome IT operations or burned by a costly security event.

The Mobile Device Landscape

The ESG data clearly indicates that mobile devices have become pervasive: in 44% of enterprise organizations, at least half of all employees use their mobile devices to get their jobs done. Note that more than 75% of employees use their mobile devices for day-to-day productivity at nearly one-fifth of all large organizations (see Figure 1).

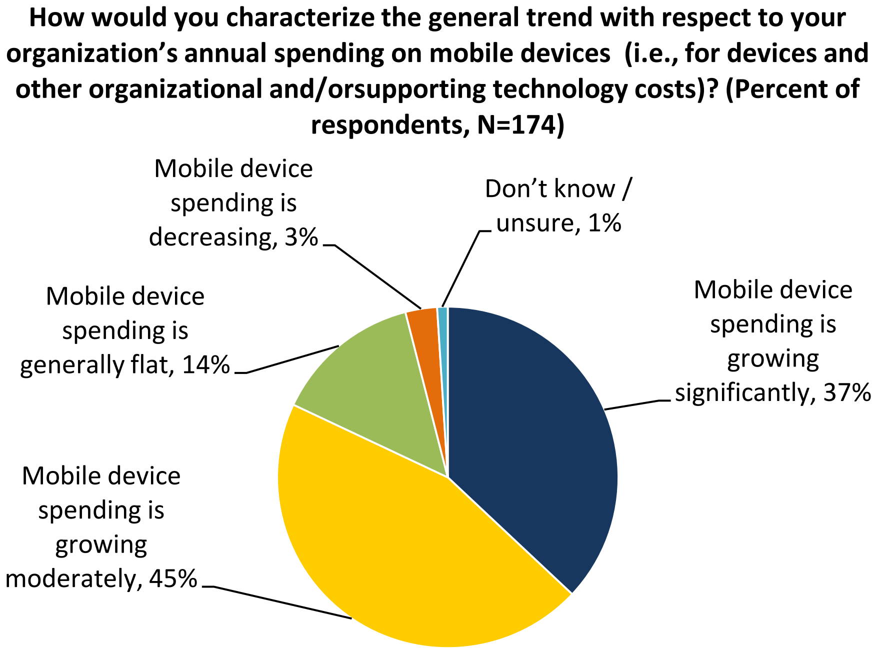
Figure 1. Most Employees Use Mobile Devices for Work at Large Organizations



Source: Enterprise Strategy Group, 2010.

Large organizations are also spending more budget dollars on mobile devices as well as the people, processes, and technologies used to manage, support, and secure them. Eighthly-two percent claim that mobile device spending is increasing and 37% of all large organizations are spending significantly more on mobile devices (see Figure 2).

Figure 2. Enterprise Spending on Mobile Devices

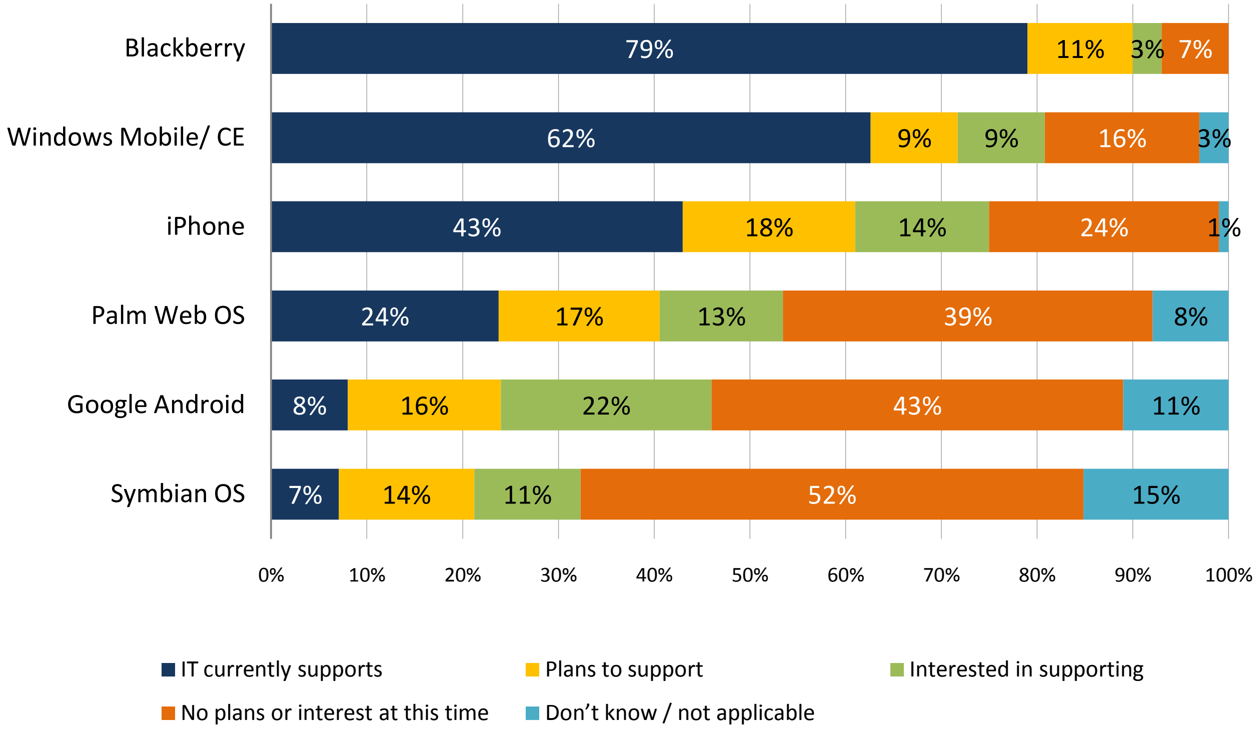


Source: Enterprise Strategy Group, 2010.

Unlike PCs, mobile devices are brought into the enterprise by individual employees. Indeed, they have become the ultimate consumer device forcing IT managers to support the trendy "phone du jour." While Blackberry and Windows mobile top the list of supported devices, Apple iPhones and Google Android phones are gaining momentum (see Figure 3). Of course, the next challenge will be support for iPads and other tablet PCs to follow.

Figure 3. Mobile Device Platform Support

Which of the following mobile device platforms does your IT organization formally support? (Percent of respondents, N=174)

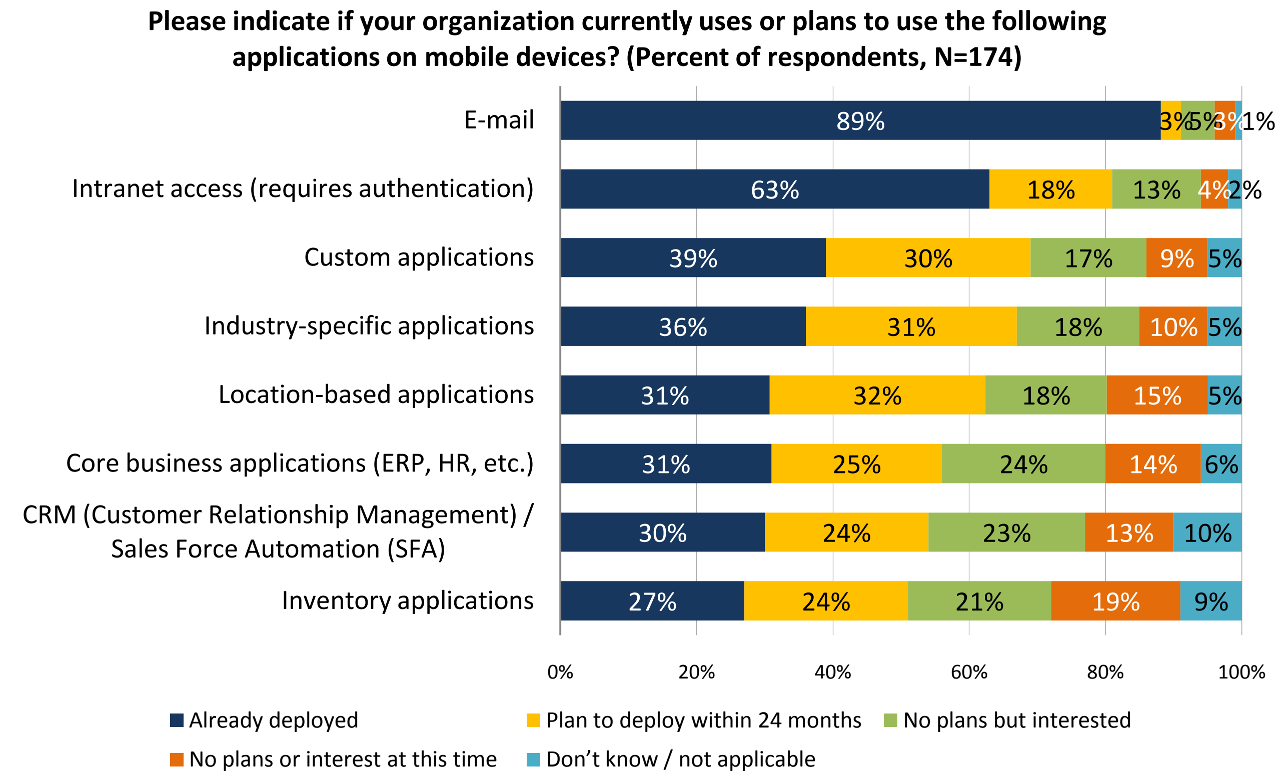


Source: Enterprise Strategy Group, 2010.

Mobile Device Use

As far as mobile device usage goes, e-mail remains the most popular application, but 63% of large organizations provide mobile device access to internal networks and portals and 30% of enterprises also offer CRM, core business applications, location-based applications, industry applications, and custom applications (see Figure 4).

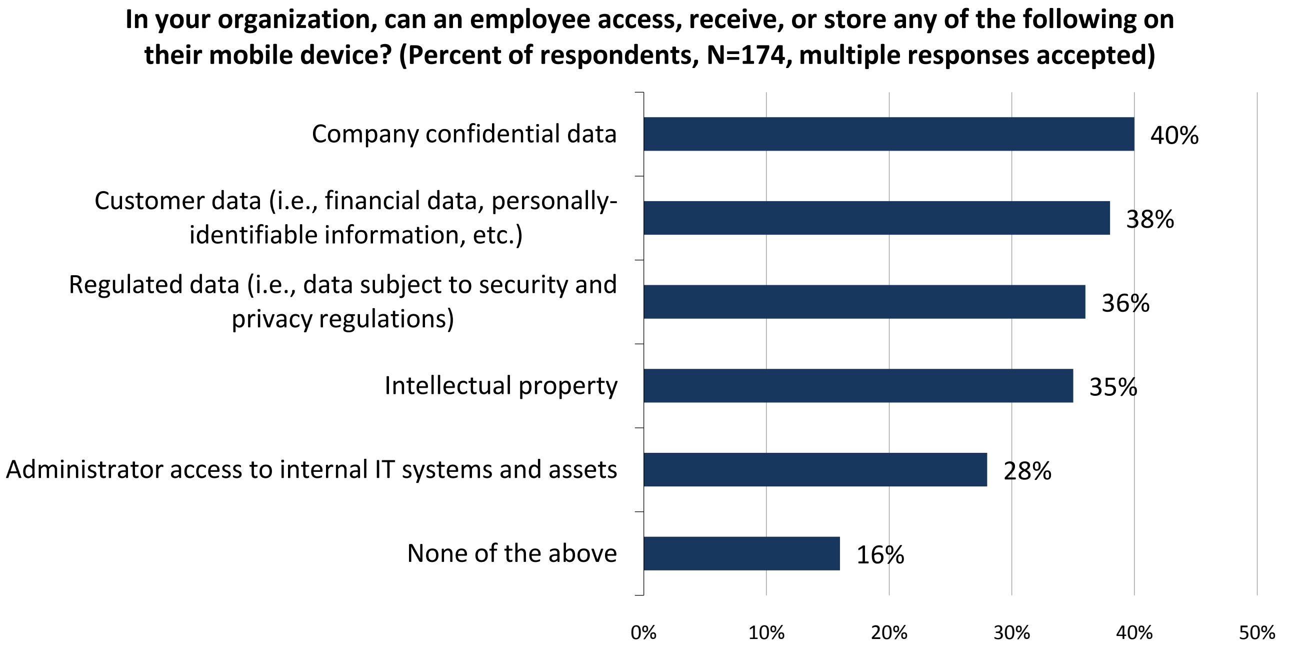
Figure 4. Mobile Device Application Support



Source: Enterprise Strategy Group, 2010.

Employees can also access an assortment of data from their mobile devices and some of this data is classified as confidential and/or private. More than one-third of respondents say that employees using mobile devices can access, receive, and/or store company confidential data, customer data, regulated data, and intellectual property (see Figure 5).

Figure 5. Confidential Data Entitlements Using Mobile Devices



Source: Enterprise Strategy Group, 2010.

The data paints a distinct picture: mobile devices are used by more employees for many types of applications and data—including confidential data—then ever before. Thus, it is no surprise that 38% of respondents said that mobile devices were "critical" for business processes and productivity.

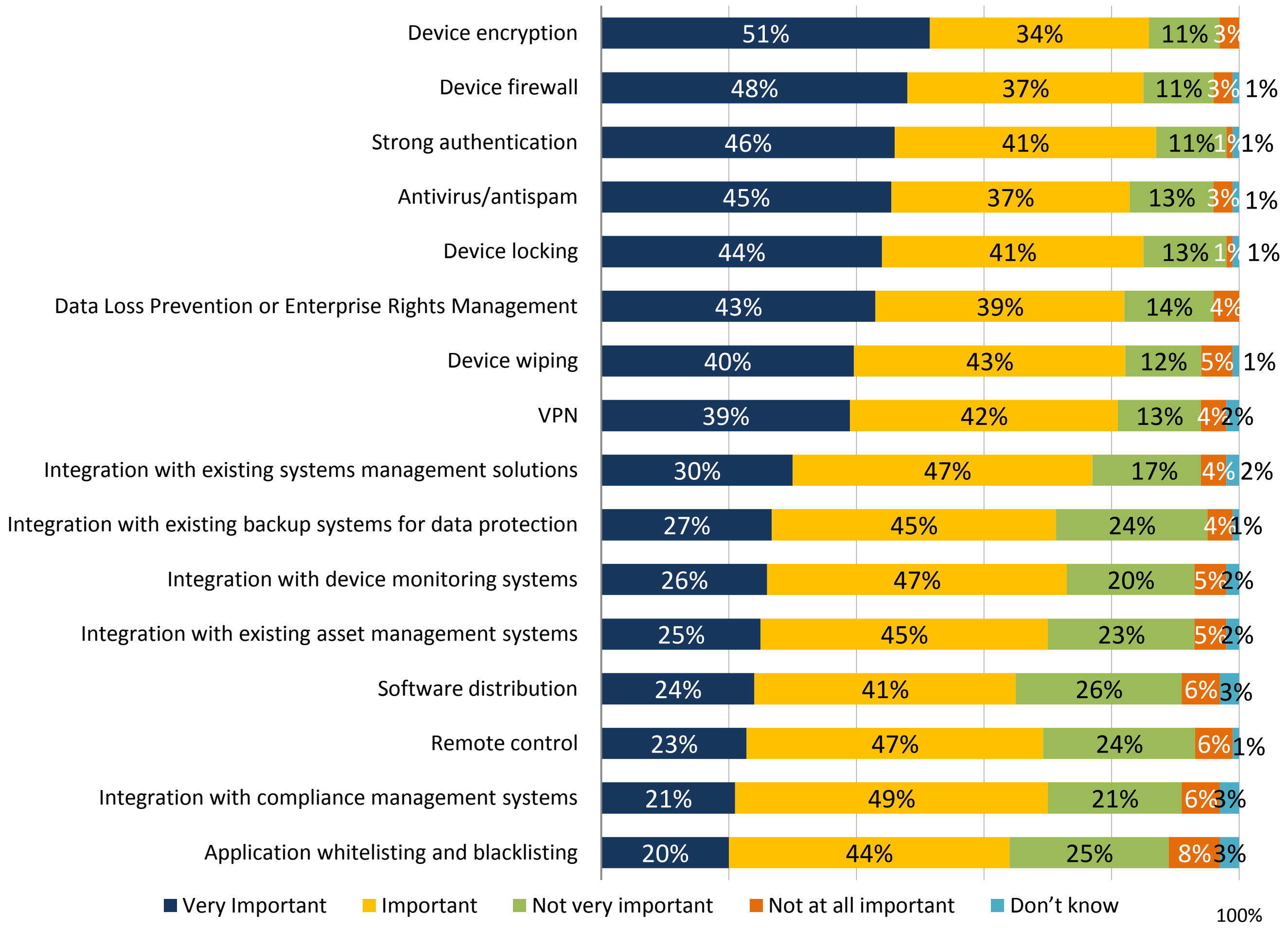
Mobile Device Security

Mobile device productivity comes at a price: increased security risk. Mobile applications create yet another path into enterprise networks, which could allow them to propagate malicious code, a scenario presented in the recent Cyber Shockwave exercise. Sensitive data stored on a mobile device could be lost or stolen, leading to data breaches, compliance violations, and expensive/embarrassing public disclosure.

Large organizations recognize mobile device threats and vulnerabilities and understand that they need proper security protection. Just what types of security controls are needed? Enterprises have a laundry list of important requirements (see Figure 6).

Figure 6. Mobile Device Security Priorities

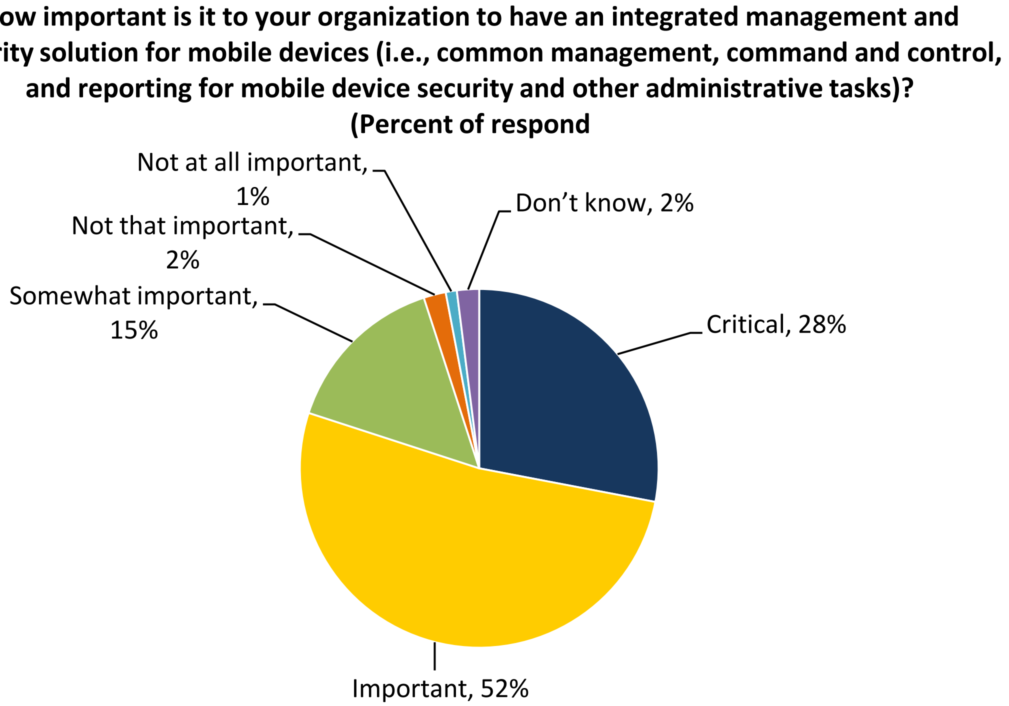
How would you rate the importance of the following features and/or capabilities when it comes to evaluating, selecting, and implementing mobile security and management technology solutions? (Percent of respondents, N=174)



Source: Enterprise Strategy Group, 2010.

Enterprises also see that mobile device security goes hand-in-hand with IT operations. In fact, 80% of organizations believe it is "critical" or "important" to have integrated mobile device security and management solutions (see Figure 7).

Figure 7. Mobile Device Security Priorities



Source: Enterprise Strategy Group, 2010.

Analysis and Recommendations

Large companies are buying mobile devices, providing mobile devices application access, and even developing new mobile device applications. CIOs must quickly recognize the growing value of mobile devices and support these mission critical business tools with IT best practices for management, administration, and security. To achieve these objectives, large organizations should:

- **Address specific needs for mobile devices.** ESG believes that Figure 6 can be used as a guideline for mobile device security and management priorities as follows:
  - **Address mobile data security.** Since users can access and store sensitive data with local devices, data security must take precedence. ESG suggests that large organizations review and update data privacy policies to include mobile devices; train users on policies, security threats, and penalties; and lock down devices with strong authentication, data encryption, and device/user behavior monitoring. Don't forget mobile device remote locking, data wiping, and backup/restore since it is likely that lost devices pose the greatest security risk.
  - **Address device security.** Since these devices will access corporate networks, they should be treated as a potential threat vector. ESG recommends that enterprises configure devices for security, apply patches in a timely fashion, train users on risky behavior and social engineering attacks, and install endpoint security that includes antivirus, firewall, Web threat protection, and application white listing.
  - **Consider mobile VPN needs.** The last thing the VP of Sales wants is complex network access controls that preclude field reps from uploading purchase orders on the last day of the month. To satisfy security and business needs, mobile security solutions should provide for secure connectivity to specific networks assets while remaining transparent to end-users.
  - **Establish good procedures and tools for device management.** This includes IT best practice frameworks like ITIL, COBIT, and NIST-800. It also means good management tools for device procurement, configuration, change management, remote support, and retirement.

- **Look for integrated mobile device management and security tools.** As Figure 6 clearly indicates, large organizations want integrated solutions for mobile security and management, not a bunch of tactical point tools. Look for integrated solutions that 1) integrate with network access control and VPNs, 2) provide a potpourri of security/management features and rich functionality, and 3) support all popular mobile devices with a broad range of functionality for each.
- **Think in terms of "lifecycle management**." Large organizations should think of mobile device lifecycles from "cradle to grave." This lifecycle will require mobile device procurement, configuration, change management, patch management, security event management, and constant health and security monitoring. In this way, IT managers can ensure that devices and users are productive, up-to-date, high performing, and safe. Remember to plan for these lifecycle requirements up front before investing in any mobile device management or security products.

The Bigger Truth

The business value of mobile devices really dictates that IT executives create an enterprise-class mobile device management and security strategy built around well-understood IT best practices. The ESG data suggests the need to prioritize security, choose integrated management and security tools, and lean on existing IT operations and management models. Working with established vendors will certainly help IT executives accomplish these objectives.

CIOs must internalize the ESG data presented in this paper and then act quickly to address risks. Remember that:

- **Mobile exploits are already happening.** For example:
    - In late 2009, researchers at several security firms reported that an iPhone worm called "Ikee.B" or "Duh" was proliferating using the default password for an application. Once an iPhone is compromised, the worm grabs text messages and searches for banking authorization codes used by at least one bank before sending the codes to a central server.
    - In September 2010, Adobe announced a vulnerability in the Flash 10.1 runtime engine that could allow an attacker to take control of affected systems, including mobile devices running the Google Android operating system.
- **A high percentage of mobile devices access and/or store sensitive data.** This means that a lost or stolen device worth a few hundred dollars could lead to a multi-million dollar data breach.

Smart organizations will recognize that security issues like these will only get worse and seek out mobile device security and management solutions in order to lower risks and streamline IT costs as soon as possible. Laggard firms that delay implementation of mobile device security will face higher risks and operational overhead—if they are lucky. Unlucky organizations may also experience security events emanating from once innocent cell phones and PDAs.

Enterprise Strategy Group | **Getting to the bigger truth.**