

# Mobility Advantage: Why Secure Your Mobile Devices?

## TABLE OF CONTENTS

	Mobile Insecurity — The Elephant in the Room
1	Understanding Mobility Risks and Remedies
1	Risks related to lost and stolen devices
2	Unauthorized data access
3	Risks related to personal and business use on the same device
3	Gaps in device management and policy enforcement
4	Life-Cycle Approach to a Mobile Security Strategy
5	Mobile Security as a Way of Life
7	Notes

### MOBILE INSECURITY — THE ELEPHANT IN THE ROOM

Industry experts say that by 2013 there will be 1.2 billion mobile workers worldwide.<sup>1</sup> They also report that by 2013, 75 percent of all U.S. workers will be mobile<sup>2</sup>, meaning those workers will use a mobile device for at least 20 percent of their work.

Another survey reveals that 36 percent of cell phone owners have either lost a phone or had one stolen.<sup>3</sup>

These facts suggest that in the near future, nearly 25 percent of all workers will have lost a mobile device that could provide access to confidential information. It's no wonder that mobile device security is a top concern for businesses today.

And yet for all that worry, few organizations devote adequate attention to mobile security. Surveys show that although mobile security is top of mind and many companies experience frequent data breaches, companies implementing a strong mobile security strategy are in the minority.<sup>4</sup> Why haven't organizations been more aggressive about securing their mobile devices? There are a number of reasons:

- The speed with which new generations of mobile devices have come into the workplace has caught many businesses unprepared;
- Work groups and employees are driving today's business mobility, not corporate IT policy makers. This has resulted in a piecemeal approach to mobile security;
- Today's mobility is complicated by workers using their own devices for both work and personal purposes;
- Security is further complicated by the increasing diversity of mobile devices in the work place;
- Easy access and a proliferation of mobile applications makes security management appear to be a daunting task.

Many companies have not implemented a comprehensive mobile security strategy because they believe it will be too costly and cumbersome. Meantime, mobility continues to become a larger part of daily business operations. And the costs related to security breaches are high. In 2009 the average per-incident cost of a data breach was \$6.75 million.<sup>5</sup>

Most companies have security policies. The challenge they face is a two-part problem:

1. Adapting security policies to a mobile work environment;
2. Deciding what kind of technology they need to manage devices and enforce policies.

The first step in building a mobile security strategy is understanding the nature of the threat.

### UNDERSTANDING MOBILITY RISKS AND REMEDIES

Indirect costs associated with security breaches are often far greater than the direct costs of mitigating damages. Beyond costs of data remediation and possible fines for compliance rule violations, security breaches can cost companies their competitive advantage. They can embarrass companies or key people in those companies, creating bad publicity and legal problems. They can cause a loss of customer and partner confidence. Ultimately security breaches can damage a company's brand and its ability to do business.

As mobility becomes a more important part of routine operations, companies who are developing a mobility strategy must address the issue of mobile security. To do that, it's important to understand the vulnerabilities.

Broadly speaking, there are four areas of vulnerability in mobile business operations:

- Lost or stolen devices
- Unauthorized data access
- Risks arising from combining personal and work use in one device
- Gaps in device management and policy enforcement

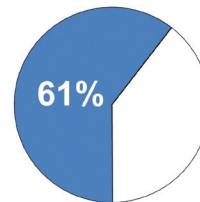
Let's look at each of these.

#### Risks related to lost and stolen devices

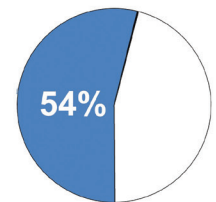
Mobile devices are easy to lose, and that is not going to change. Lost devices account for a significant amount of lost data.

In spite of the amount of data lost through stolen devices and the ease with which these devices are lost, in many cases nothing is done to actually protect data on mobile devices. The same study that found more than one third of cell phone owners in the U.S. had a lost or stolen phone also revealed another startling fact. Almost 90 percent of those people had no way to either remotely lock their devices or remotely wipe data from them. Additionally, more than half of smartphone users did not use any password protection on their phones.<sup>6</sup>

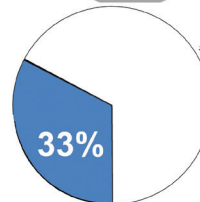
### Based on recent surveys.....



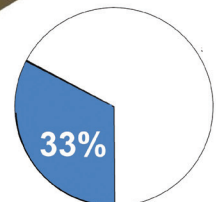
**Report that business use of smartphones is their top security concern.**



**Report at least one security breach in the past year.**



**Report requiring advanced authentication for corporate network access.**



**Report using data encryption on mobile devices.**

These facts suggest four capabilities that should be at the heart of any mobile security strategy:

- **User authentication at the device level** — This requires mobile workers to have password logins in order to access company applications and data.
- **Remote lock and wipe** — This enables companies to remotely disable mobile devices so no one can use them, and to remotely wipe data from devices.
- **Data encryption** — In case the loss of a device is not immediately discovered, any business data it contains should be encrypted.
- **Data control** — If a user does not log into the network within a certain amount of time, the device will delete its own data or block access to corporate email.

#### Unauthorized data access

This threat involves apparent authorized use of mobile devices to gain unauthorized access to data. This is not strictly a mobility issue. These same threats come from any client computing system in an organization. Mobility management tools offer ways to extend standard security policies to the mobile environment.



There are three principle ways mobile devices can act as portals for unauthorized access to proprietary information:

- **An unauthorized user accesses data with a lost or stolen phone** — User authentication, remote lock and wipe, data encryption, and data control protect against this threat.
- **Authorized users gain unauthorized access to, or make inappropriate use of, proprietary information** — This is a threat common to any client system in the organization. The added risk in a business mobility environment comes from some of the very benefits mobility provides: any time any place access, and convenience.

#### AMAZING FACTS

- Approximately 1.3 million mobile phones are stolen each year, just in the UK<sup>7</sup>
- Major US corporations lose by theft 1,985 USB memory sticks, 1,075 smartphones, and 640 laptops, every week<sup>8</sup>
- 120,000 cell phones are left in Chicago taxi cabs each year<sup>9</sup>
- In the US, 113 cell phones are lost every minute<sup>10</sup>

Security best practices, including group policies and access restriction policies, will help regulate access to proprietary information in a business mobility environment. However a mobile security strategy can provide some additional controls, including:

- **Mobile application provisioning** — Organizations control who can run enterprise applications. This provides a layer of “hard” control over access to proprietary information.
- **Remote configuration updates** — The ability to remotely adjust device settings and restrictions “over the air” ensures enforcement of established policies.
- **Event and activity monitoring and logging** — Activity monitoring and logging can quickly identify security issues and automatically control access to corporate data.

### Risks related to personal and business use on the same device

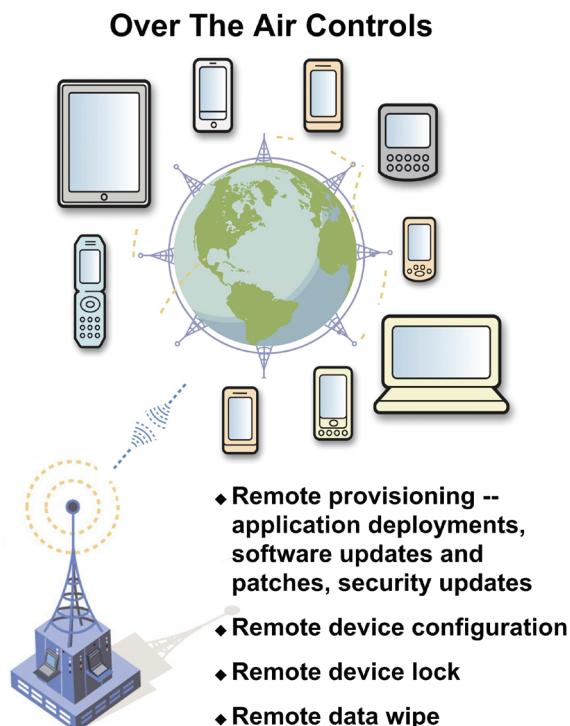
There are significant advantages to businesses that allow their workers to use one mobile device for both work and personal purposes.

Workers who can work with their preferred devices are more likely to use mobile business applications simply because it is easier for them to do so. Also, allowing employees to work with their own devices significantly reduces the company's hardware refresh costs.

However there are risks as well. Companies are rightfully concerned about any liability they may have if workers use their phones inappropriately. Also, what happens to all that data if an employee leaves the company or sells their old phone on eBay?

A mobile security strategy that includes policies and device management tools can provide controls to address these issues.

- **Segregating business functions on the mobile device** — Mobile security management tools enable companies to designate which applications and data on the devices are business related and therefore under their control.
- **Remote data wipe** — This enables organizations to enforce device decommissioning policies. For instance, if an employee leaves the company, their device can be selectively wiped of only business applications and data. This would happen without affecting “personal use” functionality. The same capability works to enforce policies so that all business information is removed from any device when it is taken out of service.
- **Data fading** — Devices not connected to the network will automatically lose their data after a period of time.



### Gaps in device management and policy enforcement

Security policies are only as good as an organization's ability to enforce them, and today's business mobility presents a challenging enforcement environment. Several factors contribute to this:

- Mobile devices are rarely physically present when it comes time to secure them;
- Most large companies support a number of different device types such as smartphones, tablets, laptops, PDAs and others. Many of these devices run on different operating systems, and new types of mobile devices are regularly coming to market.
- As business mobility becomes a more significant part of routine operations, companies are supporting larger numbers of mobile applications, each with its own data access capabilities and security protocols.

In an effort to monitor devices and enforce security policies, many organizations have adopted a patchwork collection of management and security tools. This approach is an invitation to inconsistent levels of protection.

- **A single security management platform** — This provides a common security management console capable of supporting all the device types and applications that make up a dynamic business mobility environment.

To summarize specific risks and remedies...

RISK	REMEDIES
Data lost due to lost or stolen devices	<ul style="list-style-type: none"> <li>• User authentication at the device level</li> <li>• Remote lock and wipe</li> <li>• Data encryption</li> <li>• Data control</li> </ul>
Unauthorized user accesses data with a lost or stolen phone	<ul style="list-style-type: none"> <li>• User authentication at the device level</li> <li>• Remote lock and wipe</li> <li>• Data encryption</li> <li>• Data control</li> </ul>
Authorized user gains unauthorized access to, or makes inappropriate use of, proprietary information	<ul style="list-style-type: none"> <li>• Security policies</li> <li>• Mobile application provisioning and settings</li> <li>• Remote configuration updates</li> <li>• Event and activity monitoring and logging</li> </ul>
Risks arising from combining personal and work use in one device	<ul style="list-style-type: none"> <li>• Security policies</li> <li>• Segregating business functions on the mobile device</li> <li>• Remote data wipe</li> <li>• Data fading</li> </ul>
Gaps in device management and policy enforcement	<ul style="list-style-type: none"> <li>• A single security management platform</li> </ul>

With these risks and remedies in mind, it's now possible to think strategically about mobile security. But how does one go about building a coherent strategy across all levels of an organization when today's mobility is characterized by such a diversity of mobile device types and use case scenarios?

One good way to do this is to organize security management practices around phases of a device's life cycle. Let's see why.

#### LIFE-CYCLE APPROACH TO A MOBILE SECURITY STRATEGY

There is good reason to look at overall mobile security from a device life-cycle perspective. This is because different points in the life cycle provide practical opportunities to enforce security policies.

All mobile devices have pretty much the same life cycle, which can be broken down into these phases:

- **Provision phase** — This is the time when a device is first brought into business service. Whether it is a business issued device or a personal device that is being enabled for business use, this is the best time to configure for security through the rest of the device's service life. Device "initialization" could include segregating business and personal functions, installing antivirus software, provisioning with a basic set of business applications, provisioning with data, configuring corporate email, setting up password protection, and configuring network access. This can all be done remotely using over-the-air controls.
- **Production phase** — Once a mobile device is properly configured, it is ready for business use. At that point it becomes an operational matter to keep the mobile device updated with the latest security and software patches, install or update applications as required, and monitor usage. Using over-the-air controls to perform these functions more effectively manages and protects data during the device's serviceable life.
- **Decommission phase** — This is the point when a device is retired from service. It could happen when it's time to replace the device with a newer model, or when an employee leaves the organization, or if a device is lost or stolen. Decommissioning involves removing all business data, applications, and functionality from the device. This can also be done remotely through over-the-air controls. It's possible to configure devices so they wipe their own business data and functionality under certain circumstances, for instance if they fail to log into a company network for a prolonged period of time.

#### Provision

- Establish security policies
- Initialize password(s)
- Install and encrypt data
- Install and configure anti-virus software
- Install and configure firewall and peripheral controls
- Install and configure business application(s)



#### Production

- Software and configuration updates
- Back-up device data
- Apply patch and security updates
- Enforce security policies
- Monitor and track security violations and threats
- Compliance activity logging

#### Decommission

- Disable lost or stolen device
- Wipe business data and applications from device
- Remote kill and lock
- Access violation lock
- Data control
- Disable network and application access

The key to developing and effectively enforcing a mobile security strategy is using the right device and security management tools. Many organizations have boxed themselves into a corner because of their piecemeal approach to business mobility. This is understandable, but there is a better way.

#### MOBILE SECURITY AS A WAY OF LIFE

In recent years, new mobile technology has inspired many business mobility initiatives. By providing better information whenever and wherever it's needed, mobility streamlines and accelerates business process, enables businesses to deliver better service, and provides significant competitive advantages.

These benefits, combined with the low cost and ease of adopting "out-of-the-box" point solutions, have resulted in many pilot programs and work-group level adoptions. One indicator of how fast mobility is entering the work place is the interest companies have in Apple's iPad. Less than one year after the initial release of the iPad, 80 percent of Fortune 100 companies were deploying or piloting these devices<sup>11</sup>, making this one of the fastest technology adoptions in business history.

Many business mobility applications prove very popular with workers, and once they have them, they find they can't live without them. Too often, however, good business mobility ideas turn into management nightmares. A few successful deployments create demand for more. Soon IT management is struggling with multiple mobile applications running on different mobile device types, each with its own set of management and configuration tools.

There cannot be a coherent, reliably enforceable, mobile security strategy without a single security platform used to manage all mobile devices (tablets, smartphones, laptops, PDAs, and other devices). What are the key capabilities that a mobile security platform needs to have?

- **The platform must support a broad spectrum of mobile devices** — this is important because the evolution of mobile technology is accelerating. New devices with new capabilities are coming to market. New form factors more suited to specific business applications are appearing (tablets for instance). If organizations are going to avoid becoming locked into using obsolete or limited technology, they must be able to enforce their security policies across a broad spectrum of device types. This includes being able to accommodate new mobile technologies.
- **The platform must support strong user authentication** — this is the front-line defense against unauthorized use of a mobile device.
- **The platform must support strong encryption** — this is one of the most important tools for securing data on mobile devices.
- **The platform must have the ability to set access restrictions and security policies for all mobile business applications** — this is essential in order to uniformly manage and enforce policy, and therefore minimize vulnerabilities, for mobile business operations across an organization.
- **The platform must support strong “over-the-air” controls like remote provisioning, remote device configuration, remote device lock, and remote data wipe** — a necessity for controlling mobile devices which are typically widely scattered, not conveniently retrievable to a service center, and often lost or stolen.
- **The platform must have a depth of sophisticated security controls and activity monitoring capability** — this is essential to support the same level of rights access management that large organizations require of their mainstream client computer systems.

Implementing an effective, platform-based mobile security strategy strengthens an organization's compliance with rules pertaining to protection of confidential information, lowers the incidence of data breach from mobile devices, and simplifies security management.

For more information about building secure and manageable mobile solutions, go to <http://www.sybase.com/mobilize/strategic-mobility> or contact a Sybase or SAP representative.



## NOTES

1 Garrestson, Rob. "IDC: Mobile Workers Will Pass 1 Billion in 2010." *CIO Zone*. February 24, 2010.

2 Ibid.

3 Maurer, Allan. "More than a third of consumers have had cell phones lost or stolen." *TechJournal South*. February 8, 2011.

4 Waltz, Martha. "Mobility Threats." *Mobile Enterprise*. March 7, 2011; Info security. "40% of businesses looking to deploy mobile data encryption." June 25, 2010; Check Point. "Check Point Survey Reveals Growing Mobile Workforce Expected to Increase Security Complexity in 2011." December 7, 2010.

5 Sinrod, Eric. "Data Security Breaches Cost Real Money." *FindLaw*. February 2, 2010.


6 Garrestson, Rob. "IDC: Mobile Workers Will Pass 1 Billion in 2010". *CIO Zone*. February 24, 2010.

7 Info security. "40% of businesses looking to deploy mobile data encryption." June 25, 2010.

8 Lennartsson, Kurt. "How to Use Data Encryption to Secure Mobile Business Data." *eWeek*. January 14, 2010.

9, 10 MicroTrax (2011), "Alarming Statistics."

11 Dignan, Larry. "Apple's enterprise mojo by the numbers." *TechRepublic*. January 19, 2011.



For information on our comprehensive  
Consulting and Education Services to  
support your Sybase technology initiatives,  
visit us at [www.sybase.com/consulting](http://www.sybase.com/consulting).

SYBASE, INC.  
WORLDWIDE HEADQUARTERS  
ONE SYBASE DRIVE  
DUBLIN, CA 94568-7902  
U.S.A.  
1 800 8 SYBASE

[www.sybase.com](http://www.sybase.com)

Copyright © 2011 Sybase, Inc. All rights reserved. Unpublished rights reserved under U.S. copyright laws. Sybase and the Sybase logo are trademarks of Sybase, Inc. or its subsidiaries. ® indicates registration in the United States of America. SAP and the SAP logo are the trademarks or registered trademarks of SAP AG in Germany and in several other countries. All other trademarks are the property of their respective owners. 04/11

**SYBASE®**  
An **SAP** Company