White Paper

10 Steps to Mobile Security

November 2006 — J. Gold Associates

Sponsored by:

J. Gold Associates

SYBASE iAnywhere

TABLE OF CONTENTS

Introduction

Nearly daily reports of lost or stolen mobile devices containing sensitive data has heightened awareness of the need to secure mobile devices of all types (e.g., notebooks, personal digital assistants, smart phone converged devices, portable storage device, etc.). Indeed, data escaping the company boundaries and thus exposing customer records, financial information, personnel files, etc., are not only damaging to company reputations, but can lead to real financial loss through lawsuits, regulatory fines, customer retention failures, loss of good will, etc. The lack of sufficient mobile security has reached epidemic proportions that companies must rectify quickly if they are to remain in control of their most precious asset: corporate data. Failure to do so will cause companies great harm and ultimately, may even lead to their failure.

If security is breached at your company, will you even know? Many companies have lost data that has gone unnoticed and/or unreported. Is your company one of them? While the risk of a security breach is high, the good news is that there are many ways for companies to mitigate the risks and provide a safe environment for their data while taking into consideration the diverse needs of an increasingly mobile workforce. And this can be accomplished at a reasonable cost and without any extreme efforts required from an already burdened IT organization. With data loss on the rise, penalties increasing, and a growing proliferation of mandates and regulations from state and federal governments almost assured, now is the time for companies to take action to formulate and deploy a mobile security strategy.

Are You Exposed

Nearly every company of virtually any size, from the huge multinational corporation to the small to medium business, is at risk of security breach as a result of the increasing use of mobile technology. We expect greater than 50% of enterprise computers being deployed to end users to be notebooks within 2-3 years. Companies are rapidly transitioning from their current fixed desktop devices due to an increasingly mobile and diverse workforce which often is not located within the physical brick and mortar boundaries of a traditional company setting. Further, we expect greater than 85% of knowledge workers to acquire a smart device (e.g., smart phone converged device) within the next 2-3 years as the usefulness of these devices increases beyond simply phone calls and email to be more computer-like and application friendly. This process is accelerating as prices decline, with devices of substantial capability available at under $200, and as devices become more integrated into corporate back office systems (e.g., sales applications, CRM, field forces, asset tracking, expense reporting, order placement/query, business intelligence, etc.).

Despite this dramatic increase in mobile devices, we see a substantial shortfall in many companies in both awareness and in concrete actions taken to minimize or eliminate mobile security threats and risk. Indeed, our research indicates that fewer than 10% of companies currently deploy mobile security suites, although such security suites have been shown to be highly effective in stemming data loss. And even fewer provide mobile device antivirus to anything other than laptops. Finally, few companies (<5%) are enabling VPN connectivity to non-Windows OS smart devices for mobile workers despite their substantial growth among users.

Although no security scheme is completely foolproof, companies deploying mobile security suites report dramatically fewer data exposure issues than those that do not. Further, such suites enforce security policies on users who are often lax in their "personal security hygiene". Indeed, our research indicates that left to their own initiative, fewer than 5% of users employ even such minimal security processes as turning on password protection for their mobile devices. And significantly less than 5% of companies monitor and/or trace corporate data as it makes its way from the data center to the individual users and their devices. Is it any wonder then that so many mobile data breaches occur?

Information Anywhere Suite from Sybase iAnywhere is a secure, scalable mobile software platform that addresses the converging IT requirements of enterprises today. The Information Anywhere Suite includes Afaria, a technology that provides a sweeping array of security features meant to stem the epidemic of security breaches. With Afaria, companies can be assured that users are protected and data is not exposed to security threats.

Don't expose your organization to the risk of security breaches. Afaria can help by enabling IT to manage security requirements centrally, such as enforcing power-on password, updating signature files and antivirus engines, and managing the configuration of the device. By providing management and security capabilities from a single console, Afaria can ensure security policies are enforced and devices remain updated.

The Art of Mobile Security

Companies must take concrete and immediate steps to assure protection of corporate information assets. Security must be a multi-faceted approach and encompass a variety of techniques covering the key areas of exposure. Companies should:

- **Educate every user** – the end user's "security hygiene" is the first line of defense against loss, but few companies inform and educate the end users on the proper procedures and policies to safeguard corporate assets.
- **Secure every device** – all end user devices must be brought under the security umbrella if companies are to be fully protected, including devices that users may acquire on their own initiative, whether or not explicitly allowed by the company.
- **Manage every connection** – users should not be allowed to connect to corporate networks and data centers without first having an approved, safe method of doing so. Companies must evaluate, approve and manage all methods of access.
- **Protect every piece of data** – it should be incumbent on the company to monitor and verify any data transfer to any device as serving a legitimate company or end user need, and to ensure such data is not lost or intercepted in transit. This is often the most daunting task an organization faces in securing its environment.

Don't underestimate the importance of securing mobile email. Information Anywhere Suite's OneBridge and Afaria technologies enable secure wireless email on the broadest range of frontline devices.

To assure the highest level of security, companies should deploy appropriate tools and technologies to monitor and verify. Further, there must be input as to the best methodologies from all groups that use or are responsible for managing corporate data assets, so as to formulate a security policy that provides maximum protection with minimal impact on legitimate business user needs. Any security tools and technologies should be as transparent to the end users as possible. All groups charted with securing mobile data must remain vigilant and stay informed of new and emerging threats in order to allow any remedial actions necessary to safeguard against new exposures. Finally, companies must remain flexible and continuously update their security policies and strategies to deal with new threats, but also with new business needs that may arise.

10 Steps to Mobile Security

This section provides some concrete steps companies should take to maximize security of mobile data assets. To make things easier, we have distilled the many mobile security requirements into 10 key components divided into 4 specific areas. These 10 Steps to Mobile Security include:

- **End users**
  - Set policies, document, and get user buy-in
  - Enforce policies on mobile devices for all users
- **Devices**
  - Make sure password protection is always set to "ON"
  - Include updated personal anti-virus (AV) and firewall on devices
  - Encrypt sensitive files on all devices
  - Enable device lockdown and kill
- **Infrastructure**
  - Determine what file types can be downloaded/synched by which users, when, how and to which devices
  - Log device usage for compliance where appropriate
  - Enforce connection security/VPN standards
- **Organization**
  - Review and update policies regularly, as things change often

Afaria allows IT to be in complete control of enforcing its organization's security policies, so they are transparent to the end user. This provides the maximum protection as user intervention (and potential human error) is eliminated.

Having provided an overview description of the 10 Steps to Mobile Security in brief, let's now examine them in greater detail.

Pragmatic End User Policies

The first line of defense against any mobile security breach is the end user. Each must be fully educated and informed about all policies involved in protecting company assets. The vast majority of end users will do their utmost to protect and defend companies from loss of information, and see this as part of being a good employee. However, it is appalling how few companies actually provide any education to the end user community on how best to accomplish that task. We believe companies must formulate a clear and concise mobile security policy that is communicated to all end users (key components of a sample policy appear in Appendix 1). Many companies abide by an informal policy that gets communicated in non-company sanctioned ways (e.g., word of mouth) but this is a mistake. A formal policy, taking into account realistic company needs balanced with the needs of the end user, is required. Further, such policies will form the basis for deploying security tools and technologies that can be programmed to reflect the intent of the policies and enforce the policies in an automated fashion. Such technologies can also provide transparent enforcement to the end user community who may see some of the procedures as being inconvenient and to be avoided if possible. This will largely eliminate the end user errors often associated with data breaches. Taking user intervention out of the equation is often the best policy. Once the policy is created and communicated to the end user community, it must then be fully enforced on all users, with penalties for infractions, (from minor reprimands to severe actions such as dismissal), documented and publicized.

No security tool should be deployed that is not policy driven and capable of easily allowing changes to such policies. Afaria is a policy-driven application that allows easy update and revision of custom policies through a central console, and then quickly provides those updates to all end user devices.

Taming End User Devices

Companies must define and enforce what kinds of mobile devices are acceptable to be used within the organization, and what type of threat each device represents. Unless it is a truly "dumb" device with no way of storing data, nearly all devices represent some level of exposure, and this level is rising with the increasing sophistication of even low end mobile devices. An assessment of the acceptable devices should include:

- **How each device is configured** – parameters such as password protection, network log on requirements, synchronization of files to the device, backup and recovery and applications installed, must all be evaluated and defined as part of the mobile security policy. Further, each device should contain antivirus and personal firewall capabilities to prevent data loss/exposure or infection.
- **Data transfer and protection** – defined policies should include; what types of data can be transferred to the device and from where (e.g., other device, data center), how the data is tracked and/or logged, how it is protected from exposure (via encryption), and can data be transferred off of the device (e.g., flash memory card).
- **Devices get lost but the data shouldn't** – the small form factor of many devices means portability and convenience, but also ease of loss. If the device is lost, how can it be disabled ("kill switch"), and how can a new device be configured and supplied to the end user to get back up and running quickly.

Device management and security are inter-dependent. Therefore, a combined approach is ideal for a comprehensive security solution. Afaria uniquely combines security and systems management functionality, increasing the efficiency of updating and enforcing management and security policies by enabling all necessary tasks to occur during a single connection and from a single console.

Most functions required to "tame" the end user device should be implemented within an automated process that enforces all defined policies associated with the device type, and qualified by the amount of risk associated with that device. This is an ideal area for mobile security suites, as they provide all of the capabilities associated with securing and/or locking down an end user mobile device utilizing a policy-based procedure. It is also an ideal place to deploy a more general purpose mobile management suite which includes a wide range of mobile management tools (e.g., software asset tracking, file management and distribution, license management, policy enforcement), and which compliments and enhances mobile security functionality. Indeed, a combined mobile management/security suite may be the ideal methodology to tame the proliferation of mobile devices and their associated cost to the organization.

DEVICE	THREAT TYPE	THREAT LEVEL
Notebook/ tablet	Loss/theft (device/data) Virus/worm Network compromise	**HIGH** **MEDIUM** **MEDIUM**
PDA	Loss/theft (device/data) Virus/worm Network compromise	**HIGH** **LOW** **LOW**
Smart phone	Loss/theft (device/data) Virus/worm Network compromise	**HIGH** **LOW** (short term) **MEDIUM** (longer term) **MEDIUM**
Flash drive	Loss/theft (device/data) Virus/worm Network compromise	**HIGH** **LOW** **LOW**
Portable disk	Loss/theft (device/data) Virus/worm Network compromise	**HIGH** **LOW** **LOW**
iPOD/ MP3 player	Loss/theft (device/data) Virus/worm Network compromise	**HIGH** **LOW** **LOW**

Don't Forget About Infrastructure

Most companies generally do a good job of protecting their networks and other infrastructure assets for traditional mobile workers using notebook computers. However, increasingly sophisticated mobile devices (e.g., wireless PDAs, smart phones) without complete Windows operating systems cause companies to search for alternative tools and technologies not provided by current connectivity solutions vendors (e.g., VPN, AV). Such connectivity technologies are needed to allow devices to safely access the corporate network. In some cases, companies are unable (or unwilling) to find appropriate solutions and forbid access by the unprotected devices. Companies should formulate a mobile strategy based on a variety of device types and capabilities, which should include:

- **Assuming multiple points of access** – it is increasingly likely that a single user will have multiple device types (e.g., notebook and smart phone) and access the corporate network from a variety of access points (e.g., home over WiFi, cellular network, hotel Ethernet). This proliferation of device types and access points requires companies to assure that all devices have the ability to run VPNs for access to the corporate network, and that all devices are remediated before connections (e.g., assuring AV is up to date).
- **Keeping track of portable data** – it is increasingly common for users to carry data with them on flash drives and SD cards. The low cost and high capacity of these portable storage devices makes them well suited to backing up files and moving them from machine to machine. Despite the wide proliferation of theses devices, few are protected against data loss, even though many of these small devices are lost. Companies should immediately require users to employ protected flash drives and cards that encrypt data if they are to be used for company information. Further, many security suites now include the ability to track data transferred to these devices and are a prime requirement for security and compliance regulations.

Companies must select security solutions that are able to work with the widest array of devices types and over the greatest diversity of networks. Afaria supports the broadest range of frontline devices including notebooks, PDAs, BlackBerries and smart phones. It is also optimized to run over a variety of connectivity options, including low bandwidth connections.

Infrastructure requirements should be documented as part of any security policy, and fully enforced with the appropriate technologies to assure that mobile users do not compromise the company through infection, access breaches or unnecessary copies of data.

Organizational Issues

Formulation and enforcement of a security policy within any organization requires bringing a representative portion of the entire population into the process. While IT may lead the process as the most appropriate to evaluate the technology, it is incumbent on the organization to get buy-in from a variety of groups involved in creating, monitoring and enforcement of the security policy. Representatives from lines of businesses (LOB), human resources (HR), support organizations (help desk) and potentially legal should be included in formulating a strategy so that there is no questioning or second guessing of the policy after the fact. Indeed, to best accomplish this task many companies form a Mobile Center of Excellence (COE). The COE gathers expertise from a variety of the groups, creates a policy and/or strategy reflecting the needs of corporate security across all constituencies, and obtains a management endorsement of the policy with a "stamp of approval" from the highest levels. The COE is not another corporate group in the true sense, but a virtual group of volunteers that come together for the work at hand, meet to modify the policy as needed, and offer legitimacy to the process as all segments of the organization are involved and reflected in the results. Since mobile strategies must change often as the pace of technology advances, the COE is a valuable way for companies to create, monitor and modify a complete mobile strategy, including mobile security.

Security is a Moving Target: Make it Flexible and Update Often

Companies should not assume that once created, a security policy is a fixed and/or finished document. Indeed, with the high rate of change in the marketplace (e.g., devices, connection types, applications), it is incumbent upon the organization to monitor and modify the policy on a regular basis. With the average life of a notebook of 2-3 years, the average life of a mobile phone of 12-18 months, the average life of a flash drive of under 6 months, and the vast array of new products (e.g., massive portable storage drives) and new consumer oriented devices (e.g., iPods) appearing, companies can not assume that technology will remain fixed for very long. Further, with new connectivity options, particularly in disruptive wireless technologies (e.g., WiMax, WiMesh, 3G+), users are finding new ways to get and stay connected to company information. Finally, emerging end user usage patterns (e.g., carrying data and not devices) are causing companies to reassess traditional computing models.

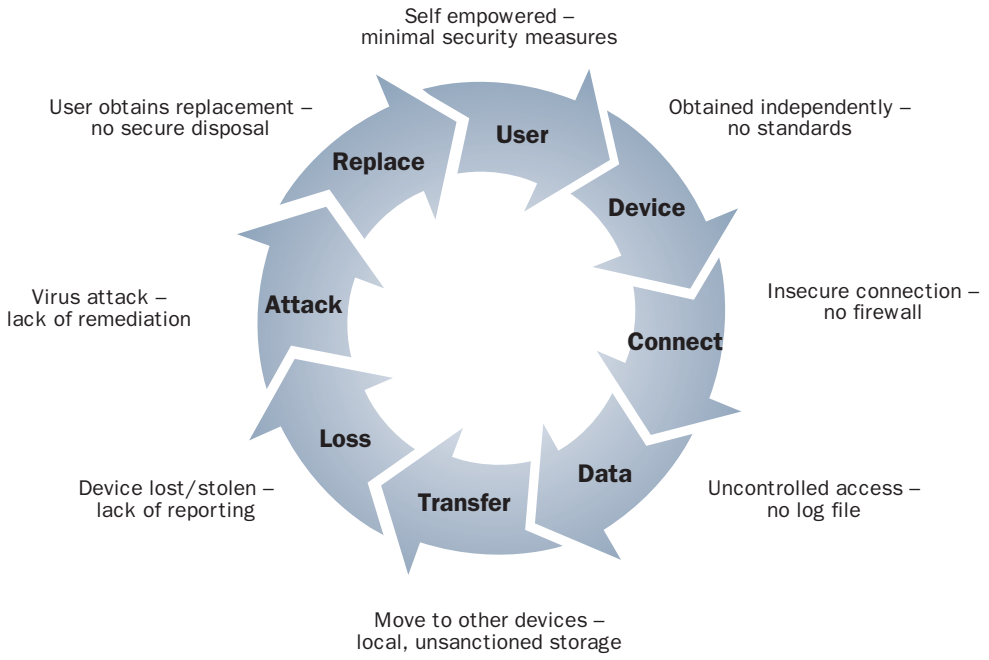
It is extremely important that companies formulate mobile security policies and standards that are flexible and that can be modified to encompass all of the emerging technologies and usage models which will appear over the next few years. Further, it is very important that companies deploy security infrastructure and technology that can be inclusive of all of these new devices, usage models, and their subsequent threats. Carefully selecting a mobile security suite and providing an ability to update and modify at will is the best insurance against early obsolescence and the need to rip and replace before the investment has been recovered. Some of the capabilities important in a mobile security suite are identified in Appendix 2.

Afaria continues to be enhanced with new device support and connection options as they become available. Further, Sybase iAnywhere will continue to enhance Afaria's ability to create, modify and deploy policy driven security capabilities to the widest array of mobile workers in an ever changing array of work styles and usage patterns.

As a leader in enterprise mobility, the experts at Sybase iAnywhere can help your company formulate a security strategy through many years of real world, hands-on experience with a variety of customers. Once formulated, a mobile security strategy can quickly be converted into a policy driven deployment with Afaria, offering the maximum protection, usability and flexibility necessary to prevent data breaches and subsequent corporate exposures.

Mobile Threat Life Cycle

Most organizations fail to fully evaluate threats from all exposure possibilities. The need to look at the entire life cycle of mobile security threats is a necessity if all bases are to be covered. The chart below represents a number of key areas companies must address. The risk and subsequent threat are indicated, but this is only a synopsis, as other threats for each category surely exist. Each company should formulate its own mobile security threat life cycle based on its understanding of its users, organization, line of business needs, and policies. It then must create a mobile security policy, and translate that policy into a programmed mobile security suite that will establish a secure environment for use by its entire mobile workforce. Failure to do so will mean an incomplete protection capability that will enable security breaches and data loss.



User Classes and Security

Most companies concentrate their efforts on securing mobile "road warriors" who are constantly mobile and who are often in the executive ranks. Yet there is an increasing class of occasional users who are also often mobile and represent a potential threat to the organization. Further, the unique needs of individual groups (e.g., executives, blue collar workers) may force security measures in a specific direction to meet those needs. Can all of the needs of all users be met with a single tool or technological solution? It is important that companies evaluate many solutions to meet the broadest needs and offer the greatest flexibility. Nevertheless, it is likely that for certain types of workers with certain classes of needs, a stand alone, best-of-breed tool will be needed to add to the capabilities of any chosen security suite. Organizations should evaluate all of the capabilities required for each class of user and then supplement any security suites as required.

WORKER	THREAT TYPE	THREAT LEVEL
Deskbound	Multiple devices Data synching/loss Virus	**LOW** **HIGH** **MEDIUM**
Work at home	Multiple devices Device loss Data loss Virus Network access breach	**LOW** **LOW** **MEDIUM** **HIGH** **MEDIUM**
Occassionally mobile	Multiple devices Device loss Data loss Virus Network access breach	**MEDIUM** **MEDIUM** **HIGH** **HIGH** **MEDIUM**
Road Warrior	Multiple devices Device loss Data loss Virus Network access breach	**HIGH** **HIGH** **HIGH** **HIGH** **MEDIUM**
Partner/ 3rd party	Multiple devices Device loss Data loss Virus Network access breach	**LOW** **HIGH** **HIGH** **HIGH** **MEDIUM**

The Information Anywhere Suite offers the flexibility needed to provide wireless email, mobile management, security and enterprise enablement to the widest array of end user requirements. Information Anywhere Suite allows your mobile deployments to expand and scale through additional interoperable technologies to meet your complete enterprise needs.

Conclusion

Satisfying corporate security needs requires a pragmatic approach that must deal with multiple elements of exposure and remediation. First and foremost, companies must develop a mobile security strategy and format a policy based upon that strategy, which then must be communicated to the end user community. Companies must take care to secure all exposure points, including user actions, user devices, all connections and access points, and any applications that might be used to create security risks. Focus must be on the entire mobile security life cycle with all of its components, rather than just a few selective areas if a realistic capability to mitigate risk is to be achieved. Companies must also not be fearful of spending on tools and technologies that can be implemented to substantially eliminate security breaches, despite most companies' lack of funds and resources for such endeavors. The relatively modest amounts spent on security tools and suites can have an enormous payback to the business in data loss prevention and its byproducts; fines, disgruntled customers and competitive disadvantage. Spending to enhance mobile security is generally a very good investment. Finally, companies must remain vigilant as threats and risks must be continually assessed and strategies changed as business and exposures change. Doing nothing to mitigate mobile security risks is a very dangerous strategy that most companies will live to regret.

Appendix 1: Elements of a Mobile Security Policy

- Who can get a device?
  - How/What type/When?
- How will the device connect?
  - Local synch, wireless?
- How will the device/user authenticate?
- What kind of data will it contain?
  - How is data safeguarded?
- What happens if device is lost/stolen?
  - How to handle backup/restore?
- What about external storage devices?
- Which apps are acceptable?
  - On device or network accessed?
- How are they protected?
- When to disable connectivity options?
  - Bluetooth, USB, IR, etc.
- What/How to remediate before access?
  - AV, VPN, Firewall, apps, etc
- How are problems reported?
  - Escalation process
- What if user fails to follow policy?

Appendix 2: Security Application Suite Requirements

Security Verification	Process Automation	Data and Content Mgmt	Connection Mgmt	System Mgmt Extension	SW Inventory Mgmt	Multi-device Support
Security mgmt • Encryption • Policy enforcement • AV/Firewall • Remote "kill" **Data backup** • Backup and restore **Patch mgmt** • Which patches/ when • Logging	**Scripting** • Files • System functions and checks **Scheduling** • Manual or auto initiated	**Document and content** • Secure delivery • Policy enforcement • Aged document removal **Data backup** • System backup and restore	**Bandwidth mgmt** • Compression • Checkpoint restart • File and byte level differencing • Dynamic bandwidth throttling • Optimized scheduling **Device monitoring** • State of device triggers • External memory logs	**Config mgmt** • Admin control of all devices • Config checking and remediation **Integration** • Integration with existing mgmt platforms (e.g., SMS)	**SW and inventory mgmt** • Automated inventories • Automatic alerts to any changes in HW/SW • Info for help desk **Remote control** • Fault diagnosis **License control and SW dist** • Detailed usage reports • Version mgmt and rollback	**Support for wide array of devices and OSs** • Notebooks • PDAs • Smart phones • Multiple OSs (Windows, WM, Palm, BlackBerry, Symbian)

About the Author

Jack E. Gold is Founder and Principal Analyst at J.Gold Associates. Mr. Gold has over 35 years in the computer and electronics industries, including work in imaging, multimedia, technical computing, consumer electronics, software development and manufacturing systems. He is a leading authority on mobile, wireless and pervasive computing, advising clients on business analysis, strategic planning, architecture, product evaluation/selection and enterprise application strategies. Before founding J. Gold Associates, he spent 12 years with META Group as a Vice President in Technology Research Services. He also held positions in technical and marketing management at Digital Equipment Corp. and Xerox. Mr. Gold has a BS in Electrical Engineering from Rochester Institute of Technology and an MBA from Clark University. He can be reached at jack.gold@jgoldassociates.com.

About the Information Anywhere Suite

The Information Anywhere Suite is a secure, scalable mobile software portfolio of products that address the converging IT requirements of enterprises today. By combining email/messaging, mobile device management, enterprise-to-edge security and back-office application extension capabilities, Information Anywhere enables organizations to empower employees to do the work they need to do anywhere, at anytime, on any device. Built from the inception to address the unique characteristics of frontline environments, Information Anywhere ensures that mobilized applications are as secure, reliable and available as those that run within the data center.

About Sybase iAnywhere

Sybase iAnywhere enables success at the front lines of business. The company holds worldwide market leadership positions in mobile and embedded databases, mobile management and security, mobile middleware and synchronization, and Bluetooth® and infrared protocol technologies. Tens of millions of mobile devices, millions of subscribers, and 20,000 customers and partners rely on the company's "Always Available" technologies, including SQL Anywhere, Afaria, OneBridge, and the AvantGo® mobile Internet service. iAnywhere is a subsidiary of Sybase, Inc. (NYSE:SY).

6 Valentine Road
Northborough, MA 01532
508-393-5294

www.jgoldassociates.com