A MOBILE ENTERPRISE WHITE PAPER

THE TOP 5 IT CONSIDERATIONS FOR SECURE WIRELESS EMAIL

SYBASE® iAnywhere®

For modern enterprises, the benefits of mobile email are clear: it's convenient, efficient, it allows for new opportunities, and it's an exceptionally effective way for workers to stay connected with both colleagues and back-office information on an always-on basis.

The security considerations surrounding this "killer app," however, are unfortunately far less straightforward. The very features that offer a boon to mobile workers are the same features threatening the safety of enterprise data and creating new challenges for technology management staffs. While IT departments have historically been responsible for evaluating devices and then securing them and their data within the four walls of a company, today those devices are on the move, putting that data in constant transit.

Heightening the need for guaranteed security further still is the exploding market of wireless push email. Push technologies—which enable email to be instantly transferred to a device the moment it's sent, versus traditional systems where email is "pulled" to the device at login and specified intervals—have caused a paradigm shift for security, as information is being delivered to devices even when they're locked. Push email is particularly complex to secure, and incompatibilities between many mobile email and security systems leave security gaps or cause corrupted data.

The increased responsibilities that mobile email creates within an IT department can hardly be over-emphasized, and these are amplified as the use of mobile email grows and as new government regulations raise security compliance standards. With customer lists, spreadsheets and other documents being sent via email, the likelihood that sensitive, government-regulated information resides on mobile devices is great. Enterprises must be securing that data, as well as be prepared to act immediately in the event of a lost or stolen device.

Complying with government mandates—and maintaining the respect and trust of customers and future customers—is, no one would argue, difficult to manage. The good news is that mobile solutions are available that can enable enterprises to confidently address each of their security concerns. Solutions from Sybase iAnywhere are among these offerings, and we'll touch on these more specifically at the conclusion of this whitepaper.

However, regardless of the vendor company you ultimately choose to secure your enterprise and its mobile data, there are five key considerations to think through first. These will help decision-makers to better anticipate their security needs, and to be sure the solution they choose to deploy is guaranteed to meet them.

1 Protect Your Mobile Assets

By their very nature, mobile devices travel. And traveling along with them are expensive and even confidential assets. It is more important than ever to seriously consider how devices and the data inside them are being protected.

The term "secure" means different things to different enterprises, and even *within* enterprises. So the first step toward devising a corporate security policy is to adequately define what "secure" means to your enterprise.

While many devices offer security features such as user name and passwords, it's naïve to treat these as fool-proof security measures. A true enterprise security solution protects mobile data—and so also the enterprise—on numerous fronts. To be sure you're not performing the digital equivalent of "locking your windows while leaving open the back door" be sure that your security definition addresses these four areas where data are vulnerable:

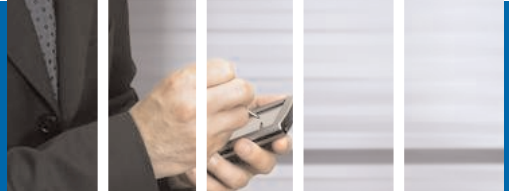
• **In Central Systems:** The internal workings of a company must be protected by following existing company security and authorization policies. For instance, while accessing a user's email inbox, it is important to use the user's credentials and not an administrative-privileged account which may lead to unauthorized abuse by disgruntled employees. Most companies may have in place an additional level of authentication for connections originating from outside the company's network. Having a system that supports a two-tier authentication is essential when dealing with mobile devices accessing corporate servers. For example, RSA security-based authentication is an example of an external authentication mechanism used by large organizations. Any mobile email system needs to comply with the existing company security policies and not circumvent it.

• **In Transmission:** Email and other data are also at risk when data is being transmitted from a server to a device and from the device back to a server. With the increasing amount of business applications being used on mobile devices—such as sales force automation tools and customer relationship management solutions—the amount and value of data traveling back and forth is considerable.

Regulated industries are especially sensitive to this issue. A good example is the Duke University Health System (DUHS), which has 11,400 full-time employees, including 5,000 physicians, researchers and faculty. In order to provide the best possible care, DUHS physicians wanted to be in constant contact with the most current patient information and lab results, as well as have access to online reference materials such as pharmaceutical and insurance formulary information.

The IT manager at DUHS knew, however, that if any of the data were accessed while in transmission it would be a security breach punishable by law, as the privacy of patient information is protected under the Health Insurance Portability and Accountability Act (also known as HIPAA). So for the DUHS IT department, part of supplying the doctors with the real-time information their jobs demanded meant also deploying a solution that could ensure the security of the data and constant compliance with HIPAA regulations.

• **On Devices:** It is imperative that organizations manage and protect sensitive information rather than leaving the burden of security to the mobile device end user. Solutions should be implemented that enable 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. Password protection is the first step toward securing data on mobile devices. Having IT determine what data to encrypt and when it should be encrypted is essential. Removable storage mediums, such as compact flash cards and SD cards, should also be encrypted. By having security policies created and controlled by IT from a



central console, mobile devices are more apt to remain in compliance with corporate security policies. This includes having the latest applications, antivirus definition files and firewall settings configured correctly and operating normally.

• **Lost or Stolen Data:** Gartner estimates more than 250,000 cell phones and PDAs were lost at airports alone last year. Studies show up to a 30 percent loss rate for PDAs. How much can it cost? After the Federal Trade Commission reported a security breach from a stolen laptop in June that put 110 million data records at risk, Congress had to earmark $160 million to fix it. IT departments should assume that at least some level of loss will come with the proliferation of mobile devices. And they should plan for securing mobile email within that environment.

Invest in technology that can instantly erase data from mobile devices if they are lost or stolen. An over-the-air "wipe" technology can completely erase a laptop or handheld that has gone missing before a thief or hacker can get by the user login.

2 Keep Your Enterprise Out of Tomorrow's Headlines

HIPAA, Sarbanes-Oxley and the Graham-Leach Bailey Act all require complete reporting and protection of financial and personal data. With so much of this data residing on mobile devices, compliance is more challenging than ever to achieve.

According to a recent research report from J.Gold Associates, a well-devised and well-executed compliance strategy is an imperative for every enterprise. Industry-based regulations, government regulations and even general business regulations can impose steep fines and even criminal liability for a failure to comply.

"The stakes are quite high," the report warns. "Besides the financial strain of hefty fines and the substantial harm to the company's reputation in the event of an enforcement action, failure to institute a compliance strategy might lead an enterprise into traps it could otherwise avoid, such as massive notification mailings to affected customers and consumers, expensive private or class-action lawsuits, or even mandatory production of a neglected 'smoking gun,' which could lead to additional enforcements."

Data security breaches may result in the loss of customer good will, the loss of competitive company data, the loss of company reputation and ultimately a loss of profit. J.Gold Associates estimates that to notify each individual whose personal data may have been exposed, as required by many current compliance regulations, would cost a company approximately $15 per individual. However, if the data includes financial information (e.g., credit card numbers), that cost rises to approximately $35 per individual. Exposing substantial records, say 100,000 users, can easily cost a company $3.5 million in notification costs alone. And this sum does not include any lost business, substantial fees or remedial measures the company must take.

Maintaining a clean reputation and avoiding fines are hardly the only reasons, though, for deploying a solution that will keep your organization in compliance with regulations. These same solutions are likely to also empower your business through increased efficiency, accountability and quality control.

While all companies, regardless of size or vertical industry, need to consider the vulnerability of their mobile email, the following industries are both particularly vulnerable and legally bound to address the issues of mobile security:

• **Public Companies:** The 2005 Specter-Leahy legislation includes criminal penalties for identity theft involving electronic personal data when it is trusted to public companies. The Social Security Act and other statutes cover this as well. No public company can afford to leave its data unprotected in a device than can be hacked, lost or stolen.

• **Government Organizations:** These have strong requirements in terms of confidentiality and security. They must adopt the Federal Information Processing Standard (FIPS) to ensure the integrity and privacy of messages from the time of origination until the time they are received and decoded by the recipient.

• **Healthcare Organizations:** Hospitals and other healthcare organizations must deal with patients' confidential information and must protect sensitive data and individual privacy. As hospitals have large campuses open to medical personnel, patients and visitors, local wireless networks are exposed to potential attacks.

• **Financial Organizations:** Financial enterprises are very careful about security issues, particularly client data confidentiality. A wireless email solution for them needs to integrate with their IT security policies to prevent external attacks that exploit weaknesses generated by wireless access.

• **Defense Organizations:** The defense industry obviously manages very sensitive information. Devices are used in hostile environments where they could be stolen or communications could be intercepted by enemies. These organizations need wireless email to have the very highest security at all levels for data servers, transmissions and handheld devices.

3 Push Email May Push the Limits of Your Security

Enterprises have instantly recognized the availability of real-time information that push email provides (versus traditional email technologies, which required an occasional refresh from the user and had built-in intervals of several minutes) as a competitive advantage in business. But again, what's a coup for end users is a new challenge for IT.

The first area of concern regarding push email is its very nature: the constant refreshment of information. In the hands of a mobile worker it's glorious; but should a device be lost, stolen or simply left unsupervised, it can be a cause of alarm. Many companies have turned to various encryption models to guard against this, and J.Gold Associates, in the same report referenced earlier, stresses concern for the data often populating mobile devices.

"Although most data streams over wireless carriers are highly secure, and therefore not subject to interception, companies must nevertheless be concerned about the devices themselves and whether or not the resident data can be easily compromised," states the report. "The rate of loss and/or theft of smart devices is on the rise. Storing sensitive data in open format is certainly not a 'best practice' for any company whose users often have highly sensitive data, including within email."

The second area of concern is the incompatibility of the different push email

offerings—and in large enterprises, or in the event of purchased or merged companies, it's not uncommon that a single company could have numerous push offerings deployed. Not all push technologies are created equal, however, and flaws have been found in some push email solutions.

For example, one company's file syncing technology can only sync to specially formatted datasets, which means that some transfers of data are performed with the data unencrypted. J.Gold Associates, reporting on this finding, writes: "This is contrary to how the major wireless email third-party applications currently perform, where all data transferred to the device is in an encrypted file format in addition to encrypting the transmissions ... although the transmission of data files across a network is secure, the storage of data files on the device is not."

The best approach is consistency. A company that uses a consistent means of encryption, a consistent means of tracking messages through servers and then a consistent security system is more likely to avoid problems with push email.

4 A Mixed Environment is a Reality at Most Enterprises

Long gone are the days when a single device populated every desktop. Today it's entirely common across a number of industries to find the employees of a single company using different devices. This may be the result of personal preferences, of specific job functions, of rankings within a company or a handful of other factors. Often, while legacy systems or offline devices still meet the needs of some, others will have transitioned to converged devices (such as the Palm Treo, RIM BlackBerry, Motorola Q and Nokia E62 among others), which combine all the functionality of a cell phone with Internet access and the most common features of a laptop.

A report from research firm IDC predicts that converged mobile devices for the enterprise present tremendous growth potential with "significant opportunities for differentiation and specialization arising from stringent IT requirements and increasing demand for additional features and functionality." IT departments need to prepare for such a future by ensuring that their security solutions match their multiple-device environments.

A 2005 Gartner report, "Key Advice on How to Support PDAs and Smartphones in Business," backs up this advice, as well as addresses a more specific model for supporting mixed-device environments. It suggests that devices be classified into three groupings: trusted, tolerated and despised. Trusted handhelds are granted privileges similar to those granted to enterprise-supported PCs and notebooks. Despised handhelds are to be kept out of the enterprise and given absolutely no support. Tolerated handhelds are granted limited privileges to provide voice communications and access to enterprise personal information management (PIM) and email, rendering them essentially fixed-function appliances.

IT departments would be wise to take an inventory of all the mobile devices being used by their employees to access and send email. Following this, it should look at the security strong points and vulnerabilities in each and address them accordingly.

5 You Can't Secure What You Can't Manage

Organizations need to develop and enforce corporate security policies across all mobile devices and applications. For email, policies should include areas such as how many days of messages should be on a device, or how frequently should users be made to update power-on passwords.

The key to maintaining those security policies is enforcing consistency, rather than developing and managing different policies for every device and operating system. It's also important that the vendor you choose to work with offers an integrated security and email solution that can manage your policies across user groups, devices, etc., from a single console. Ensure that the solution additionally offers flexibility to specific groups of users—policies may be different for executives versus remote nurses, though this depends on the type of users and the sensitivity of the data on the devices. The more flexible a solution can be to your enterprise's needs, the greater the control it will offer you.

In conclusion, don't forget that enforcing security best practices is as much about the technologies you deploy as it is about the security culture you create. Educate your employees about the importance of adhering to security policies—truly, no worker wants to be the one responsible for a data breach. And likewise, encourage IT managers to work more closely with end users and to understand their day-to-day processes, whether those end users are utility workers out in trucks or pharma reps covering three cities a day. The better that IT can relate to the work of the end users, the more likely the solutions they choose will cover every enterprise need.

Leadership in Delivering Secure Wireless Email

Ready to deliver secure wireless email to your mobile workers?

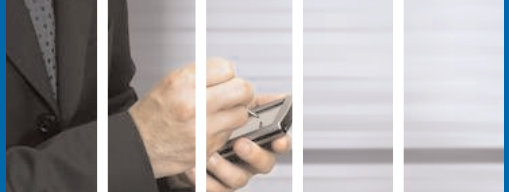
Sybase iAnywhere's award-winning Information Anywhere Suite technologies can help. OneBridge extends enterprise email (Lotus Domino or Microsoft Exchange) and applications to a more than 130 mobile devices. Tight integration with Afaria Security Manager ensures that email and PIM data is secure and never compromised.

Ensure your wireless email and other data is always secure and available anytime, anywhere. With Sybase iAnywhere, you can deliver the critical business data your users need:

- To any device, including Windows Mobile, Palm, Nokia and Sony Ericsson devices
- Using any email system, such as Lotus Domino and Microsoft Exchange
- Over any connection

Sybase iAnywhere's Information Anywhere Suite is a secure, scalable mobile software platform that addresses the converging IT requirements of enterprises today. By combining email/messaging, mobile device management, enterprise-to-edge security and back-office application extension capabilities, this suite enables organizations to empower employees to do the work they need to do anywhere, at anytime, on any device. And since it was built to address the unique characteristics of frontline environments, Sybase iAnywhere can ensure your mobilized applications are as secure, reliable and available as those that are running within the data center.

For more information about secure wireless email, please visit: http://www.ianywhere.com/swe ■



About Sybase iAnywhere

Sybase iAnywhere 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.

Contact info:
Sybase iAnywhere
Worldwide Headquarters
One Sybase Drive
Dublin, CA 94568-7902 U.S.A.

For general information:
Contact_Us@iAnywhere.com

North America
1-800-801-2069
1-519-883-6898

For specific regional product information:
Europe, Middle East, Africa
+44 1628 597 100
Asia Pacific
+852 2506 8700
Japan
+81 3 5210 6380
Benelux
+31 (0)30 - 247 8444
France
+33 (0) 1 41 90 41 90
Germany
+49 (0) 7032 / 798 - 0
United Kingdom
+44 (0) 1628 597100

SYBASE® iAnywhere®