



Defining Your Corporate Mobile Policies

It's important that corporate mobile policies cover everything from what types of devices will be available to users, how and when they can use them, what corporate resources they are able to access and what security measures will be instituted. Furthermore, Mobile managers must not ignore the impact of government regulations and compliance when laying out their corporate mobile policies. To learn more about developing appropriate mobile policies for your organization read this expert E-Guide, a compilation of trusted published SearchMobileComputing.com articles.

Sponsored By:



About Blackberry

Industry-leading BlackBerry® solutions connect people to business information, colleagues, friends and family. They offer mobile users award-winning access to email, phone, instant messaging, web, text messaging (SMS and MMS), organizer and more. Whatever your needs, there is a BlackBerry solution that's right for you.



SearchMobileComputing.com

E-Guide

Defining Your Corporate Mobile Policies

Table of Contents:

[Mobile security culture starts at the top](#)

[Defining your mobile security policy](#)

[Government regulations and mobile security policies](#)

Mobile security culture starts at the top

No business should operate today without a solid plan for the security of data on mobile devices, networks and applications. Case in point:

- Back in 2000, the CEO of Qualcomm, Irwin Jacobs, had his laptop computer stolen right off the podium where he had just finished speaking. Jacobs later admitted that the computer contained sensitive information that could be of great value to “foreign governments.” Given the venue, it’s pretty clear this particular laptop was targeted by professionals and stolen for what it contained, not just as a commodity to be fenced by common thieves.
- The Veterans Administration announced in 2006 that an employee of Unisys lost a computer that contained insurance claim data, including social security numbers, for approximately 16,000 individuals. Presumably, this computer was stolen for quick resale, and the data on it was not in this case the target of the theft—but no one can be sure that the data was not misappropriated.
- The hackers who stole the personal information of more than 45 million credit and debit card users from TJX Corporation in 2005 and 2006 used weak Wi-Fi security as their portal into their quarry. This breach, which could easily have been prevented, cost TJX hundreds of millions of dollars and an untold loss of confidence from investors, regulators, suppliers and customers.

Sad events such as these are all too common. This might sound a little extreme, but I personally find it positively criminal that such fundamental security failures arise when relatively simple and very effective countermeasures exist today—and that senior managers haven’t addressed these obvious risks not just to information security but to the business or enterprise (or even government) itself.

And IT security just isn’t that hard. Technically speaking, the core of any good security solution includes the following:

- **Strong authentication**—Users need to authenticate with their devices, and devices need to be authorized individually for network and application access. I like strong, two-factor authentication—for example, using fingerprint scanners built into mobile devices—but even a password or PIN code is a good start.
- **Data encryption**—Every security policy needs to specify that all sensitive data will be encrypted—both on mobile devices and on network servers—and available in the clear only to authorized users. No exceptions!
- **Virtual private networks (VPNs)**—Sensitive data must never appear in the clear while being transmitted across any network, whether wired or wireless. VPN technology to meet this requirement is cheap, readily available, and working in countless venues today.

So, since it’s so easy to build effective, usable security solutions, how come we still have problems like those noted above? Part of the answer here is a lack of education. IT, by its very nature, can be complex; and, especially with respect to security, one can never declare that a given solution is “done.” Effective security requires a commitment to staying up-to-date on both the constantly evolving threats and new solutions to them.

But a bigger problem is the lack of what I like to call a culture of security in most organizations. Culture, of course, is about the (sadly, usually unwritten) rules about how one relates to others within a society or organization—beliefs, customs and procedures. Good enterprise information and network security, however, require written rules (a security policy at a minimum), education and training, and, again, a commitment to establishing and maintaining effective solutions. And this culture of security must start at the highest levels of the organization, from the CEO and board of directors on down. This is, I must report, the only way to build effective IT security into enterprise operations.

OK, that's the problem. Next time we'll look at the incentives and key operational elements available to senior management in the pursuit of effective IT security. And we'll close this series with a set of recommendations that aren't hard to follow and are designed to assure the folks at the top that IT security won't be constantly at the top of their to-do lists.

About the author: *Craig Mathias is a principal with Farsight Group, an advisory firm based in Ashland, Mass., specializing in wireless networking and mobile computing. The firm works with manufacturers, enterprises, carriers, government, and the financial community on all aspects of wireless and mobile.*

Your business is
going mobile.
Are you equipped
to manage it?



The BlackBerry® Enterprise Solution provides you with tools and IT policies to keep control of your mobile deployment.

The number of mobile workers is on the rise everywhere. But with increased mobility comes the potential for increased risk, since handheld devices with sensitive data can be lost, stolen or compromised. With more than 400 published IT policies, the BlackBerry Enterprise Solution enables administrators to maintain fine-grained control over their wireless deployment—through intuitive, comprehensive IT policy management tools.

Welcome to the BlackBerry solution advantage



For more information on how the BlackBerry solution can help mobilize your business visit: www.blackberry.com/go/mobilizeyourbusiness

©2008 Research In Motion Limited. All rights reserved. BlackBerry®, RIM®, Research In Motion®, SureType® and related trademarks, names and logos are the property of Research In Motion Limited and are registered and/or used in the U.S. and countries around the world.

 **BlackBerry**

Defining your mobile security policy

A security policy is a document that defines how a given enterprise approaches the security of its IT resources. The scope here can be very broad indeed—physical security, network security, information security, and (especially important for our purposes here) mobile device security. It's very important that a security policy be in place before any decisions are made as to specific solutions—while basic security measures should always, of course, be operational, too often major and otherwise expensive upgrades are made before a real need for them has been established. A security policy therefore serves as a vital focal point for any enterprise or organization.

In general, a security policy defines what information is to be treated as sensitive (and therefore protected), who should have access to this information and under what conditions, and—very importantly—what to do when security is compromised (or even suspected of being compromised). From a physical security perspective, it should define who may have access to IT-specific areas of a given installation or building and how these areas are to be secured. But the following three elements are most important with respect to mobile security:

- **Information security**—this defines what information should be treated as sensitive. I generally recommend adopting an approach similar to that used by the government, which is to have multiple levels of security with fewer people or groups having access as the classification level rises. For example, we might use a legend of “Company Confidential” for any data that is restricted to employees, and “Company Most Confidential” for that restricted to only certain employees. This policy might also restrict access to certain applications to authorized users only.
- **Network security**—there are two key elements to the solution here, strong authentication and the encryption of sensitive data wherever it is stored. Note again that while a security policy will not usually define the actual solution in any given case, it will mention, for example, that two-factor and/or mutual authentication is required and that a VPN must be used when accessing the enterprise network remotely. It might even restrict the choice of a specific network to certain approved carriers.
- **Device security**—Finally, this part of the policy defines how security is maintained on mobile devices outside the perimeter and otherwise outside the protection of the physical enterprise. It might restrict the ability of a user to install an application on the device, for example, and it might specify that mobile devices are to be backed up or virus-checked or that a particular firewall configuration might be required. I think that eventually so much will be required of mobile devices that they will simply need to be provided by the enterprise. There's no effective way to manage security—or anything else, for that matter—on a device that the company does not own.

Each of these areas can be affected by some kind of security breach, and the security policy defines what to do when a potential (or realized) security problem occurs. For example, a lost handset might involve little more than a phone call to the team that will remotely “zap” (erase) any sensitive data on the unit, while unusual network activity might involve shutting off remote access and waking an emergency response team.

Critical to the success of any security policy is the building of a culture of security within the organization. As with those “Loose Lips Sink Ships” posters from World War II, everyone entrusted with confidential information must always be conscious of the need to protect it. The stakes today are higher than ever (and I'll expand on this next

time), so every effective policy must be backed up with an awareness campaign that includes training in both the policy and tools needed to implement and enforce it. And, again, while those tools are not necessarily defined in the policy, solutions must be convenient to use and simple enough that support costs will be limited.

Finally, keep in mind that a security policy isn't all you'll need—the security policy will need to mesh with an acceptable-use policy and perhaps also with business continuity (integrity and availability) plans as well.

About the author: *Craig Mathias is a principal with Farpoint Group, an advisory firm, based in Ashland, Mass., specializing in wireless networking and mobile computing. The firm works with manufacturers, enterprises, carriers, government, and the financial community on all aspects of wireless and mobile.*

Government regulations and mobile security policies

We'll start this column with the final major influence on an enterprise security policy—the impact of governmental and industry-specific regulations. I want to provide a little additional motivation to create and maintain your security policy—and regulation across all major industries most certainly serves that purpose. Major, widely publicized security breaches have in recent years provided significant incentive to both the regulatory community and major corporations to upgrade their security postures. Dealing with a failure in IT security can have costs far beyond the obvious need for security policy and technology improvements—the loss in customer and shareholder confidence, legal expenses, erosion of goodwill and reputation, and just the sheer volume of time that management teams must devote to damage control are major drains on market stature, competitive position and, of course, the bottom line. All of this makes getting one's security policy (and implementation) right the first time of critical importance.

The regulatory environment has become much less tolerant of IT security failures over the past few years. Here are just three examples:

- **Sarbanes-Oxley (SOX)**—SOX was passed during the era of the Enron and WorldCom scandals, primarily to address public-company accountability and openness. Interestingly, SOX does not address the issue of IT security directly, but various sections of the Act do contain wording that has been broadly interpreted to mean that organizations which do not take appropriate steps to protect sensitive information may face significant legal woes.
- **PCI**—The Payment Card Industry has set up its own standard and a set of procedures (including a detailed self-assessment) for its members. Credit-card data has been the source of a good deal of trouble for retailers in recent years, with a number of notable thefts of cardholder information. Anyone involved in retail needs to be familiar with this set of standards and guidelines; more information can be found here: <https://www.pcisecuritystandards.org/>.
- **HIPAA**—The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is designed to provide individuals with a high degree of privacy with respect to their healthcare records. IT security is of paramount importance here, and the penalties for compromised security can be severe.

But even if your business is not directly subject to these or similar security regulations, it's not a bad idea to conduct your business—and set your security policy—as if it were. The key, again, is deciding which information is sensitive, who should have access to it and under what circumstances, and what to do if this information is compromised for any reason—the core elements of any good security policy.

And once the policy is in place, most functional security solutions will consist of establishing procedures and tools for authenticating users of devices, networks and applications; authorization to use specific services; accounting to keep track of access and what was done; establishing wireless (airlink) security and network (VPN) security; and the encryption of sensitive data wherever it is stored—even on mobile devices. Strong authentication, ideally two-factor and mutual, is the best solution, and authentication deserves special attention regardless. And no matter which tools you select, be sure to review your security policy at least every six months. Unfortunately, constant awareness is essential in IT security—this is one area of IT where no one is ever “done.”

Finally, you'll note here that we focused in this series on the policies and, to some degree, the techniques of mobile information and network security, but I must confess we left out what might be the most important of all the pieces of the security puzzle: building a culture of security. And this element is so vital that we'll be devoting a series of columns to the topic in a couple of months. Stay tuned!

About the author: *Craig Mathias is a principal with Farpoint Group, an advisory firm, based in Ashland, Mass., specializing in wireless networking and mobile computing. The firm works with manufacturers, enterprises, carriers, government, and the financial community on all aspects of wireless and mobile.*