

The CIO's Guide to Mobile Security

Companies that are interested in securing their mobile workers and preventing unauthorized access to important company resources need to implement an enterprise wireless security strategy. Learn about the challenges associated with increased worker mobility and how to create an effective enterprise wireless security strategy with some suggestions for an enterprise wireless security policy.



The CIO's Guide to Mobile Security

Table of Contents

Executive Summary	2
Introduction	3
The Enterprise Wireless Security Policy	4
Securing the Mobile Device and its Data	5
Controlling Access to the Device Through Authentication	5
Security of Stored or Removable Data on Mobile Devices	5
Virus and Other Malware Protection	5
Security of Bluetooth Connections on Mobile Devices	6
Securing the Communications to and from the Mobile Device	7
Confidentiality, Integrity and Authentication Over the Network	8
Confidentiality	8
Authentication	8
Integrity	8
Optimizing the Enterprise Network to Support Business Mobility	9
Extending the Network Perimeter to the Mobile Worker	9
Segmenting the Network for Security and Reliability	10
Device Management Makes it Easy	10
Conclusion	11
For More Information	11
Related Resources	12
Appendix A - Mobile Security Checklists	13

Executive Summary

The era of Business Mobility has arrived. More workers are spending more time away from their desks doing their jobs. No matter where they are and what time of day it is, they need access to the tools and information required to help them be effective and productive.

The incredible growth in coverage of wireless networks, combined with the proliferation and increased performance of mobile devices, has given mobile workers the tools they need to make this happen. However, the potential downside is that with more mobile workers doing their jobs outside of the secure boundaries of the company, there is an increased risk of compromising data security and/or allowing malicious users access to the corporate network.

Companies that are interested in securing their mobile workers and preventing unauthorized access to important company resources need to implement an enterprise wireless security strategy. This document will introduce the challenges associated with increased worker mobility and provide simple guidelines for creating an effective enterprise wireless security strategy, including some suggestions for an enterprise wireless security policy.

Introduction

Business Mobility is growing at an accelerating rate. It is being mandated from the C-level to improve employee reachability and productivity for all levels of the organization. According to a 2008 research study, about 20% of enterprise employees in North America and Europe can be considered mobile, i.e. spend more than 20% of their time away from their primary workspace. It is expected that this number will grow to almost 60% of enterprise employees by 2012. More workers will be telecommuting, traveling and working away from their desks, but they need to maintain their “reachability” and be able to respond to customer queries the same as if they were at their desk.

Much of the incredible growth in Business Mobility can be attributed to a few notable technology trends. First is the advent of pervasive wireless. The accelerating deployment of 3G, 3+G and even 4G mobile networks, Hotspot proliferation, and the growing popularity of Wi-Fi® in the home and office have meshed to create a seamless umbrella of wireless coverage that enables the mobile worker to roam from the office to the coffee shop to the home while staying connected to a reliable, high-bandwidth network at all times. In this new era of pervasive wireless, worker location and even time of day may no longer be an obstacle to productivity and quality customer service.

Another trend contributing to the advance of Business Mobility is the growing number and capability of mobile devices. Just as many businesses are replacing their desktop computers with laptops, they are also replacing old laptops with smartphones. A recent study claims that over the next 5 years, the number of smartphones sold will exceed the number of laptops, mostly from their introduction as a laptop replacement. One of the reasons for this surge in popularity is that smartphone usage is spreading rapidly throughout the organization, moving out from sales and the executive ranks to reach the general enterprise employee. According to another study, the smartphone market is projected to grow from 10% of total handheld device sales in 2007 to over 30% in 2013.

Today’s smartphones go beyond the basics of voice and data to provide a fully-converged mobile computing platform capable of providing access to strategic enterprise applications on the go.

The smartphone of today provides the same processing performance and data storage capacity as cutting-edge enterprise desktops from a few years ago. Usability concerns are being addressed through the inclusion of space-optimized QWERTY keyboards, voice recognition and innovative haptic (touch screen) interfaces. The bottom line is that there are many more enterprise workers using increasingly capable mobile devices on wireless networks that are steadily becoming pervasive. Unfortunately, this rapid increase in Business Mobility can come with a price - an equally rapid increase in wireless security exposure.

When workers spent all of their working hours tethered to their desks, network security was easy. Network access was limited to desktop computers using physical Ethernet connections and the user was authenticated onto the network according to their username/password. These days, mobile workers can connect from anywhere in the world over public wireless networks, using anything from a laptop to a smartphone. This uncontrolled access can be an IT nightmare, as they struggle with the challenge of securing a user who is outside of the corporate network while accessing sensitive data that lies within that network. To be effective, an enterprise wireless security strategy needs to address:

- Securing the mobile device and its data
- Securing the communications to and from the mobile device and the corporate network
- Optimizing the enterprise network to support Business Mobility.

The Enterprise Wireless Security Policy

The most effective approach to ensuring enterprise wireless security is a proactive one. Most organizations implement appropriate network security measures to ensure that only authorized devices are connected to the network. These measures include standard policies that address user authentication, network security and virus protection for the wired network. When extending the organization's security policies to mobile devices, the wireless policies should support and be integrated with the existing security standards. It is important that organizations develop, educate, enforce and maintain an enterprise-wide wireless security policy. One study found that, in 87% of the cases reported in 2008, investigators concluded that the data breach could have been avoided if reasonable security controls had been in place at the time of the incident.

After the wireless security policy is developed, employees must be educated. They should be made aware of the vulnerabilities of mobile devices and the implications to the company if they fall into the wrong hands or are used in an insecure manner. Large public companies or those that operate in a regulated industry need to go beyond education; a plan for tracking, measuring and auditing its security policy performance needs to be put in place to determine if the policies are being implemented and are proving effective.

IT administrators should have the ability to mandate passwords for mobile device users and erase data from mobile devices remotely. IT administrators need the ability to establish, enforce and update mobile device settings through policies or parameters that provide comprehensive control across all mobile devices. To direct how users interact with organizational systems, administrators need a single point of mobile device management, which should reside behind the corporate firewall. This means that administrators, rather than mobile device users, determine how corporate data is protected.

Securing the Mobile Device and its Data

The most risk-prone components of any Business Mobility solution are the mobile devices themselves. Form-factor and portability, those very attributes that make the mobile device so useful and desirable, also make them prone to theft and loss. Statistics from 2008 reveal that over 5000 cell phones are left in NYC yellow taxis every month and that Disneyland finds over 300 lost cell phones every week. Stolen phones are just as common. According to a 2006 study, 9% of UK cell phone owners have had their phones stolen. That extrapolates to hundreds of thousands of mobile devices that are lost or stolen every year on planes, trains, automobiles and even roller coasters. Each device can contain sensitive company information, and potentially provide access to the corporate network.

Company information that is stored on a mobile device must be just as secure as information stored behind the firewall on the corporate network. The least serious consequence that can be hoped for when corporate data is accessed by unauthorized parties is bad press and embarrassment. However, it is entirely possible that unauthorized access of devices will result in more serious problems for the company, such as identity theft or industrial espionage. Additionally, many public companies operate within compliance and regulatory environments. For financial firms, a lost device could mean violation of the Sarbanes-Oxley Act or the Gramm-Leach-Bliley Bill, both of which mandate strict controls over disclosure of financial information. For health care companies, just the potential for unauthorized access to patient data violates the Health Insurance Portability and Accountability Act (HIPAA). Violations can result in significant fines, lost business or even forced restructuring.

Controlling Access to the Device Through Authentication

Sensitive information on a mobile device can be protected in several ways, the most common of which is user authentication through the use of an individual password. The password is designed to ensure that only the proper owner gains access to device data and functionality. Wireless security policies should mandate the use of private passwords. Ideally, password syntax should be enforceable and password expiration should be automatically scheduled so that users are required to change their passwords on a regular basis.

Organizations that are more security-conscious can require corporate wireless devices to support multiple authentication modes through the use of smart cards, biometrics or other similar mechanisms. Multiple factor authentication increases security by ensuring that access to the device requires not only something the user knows (the mobile device password), but also something the user has (for example, a smart card) or something the user "is" (for example, the user's fingerprint) that is unique to the user.

Security of Stored or Removable Data on Mobile Devices

Many wireless solutions today provide the ability to remotely erase the data from a device. However, even with a diligent user, a time lag often exists between when the user loses the device and when they contact the IT department to report the device missing. During this time period, an unauthorized user could access the device and extract valuable data. To prevent this, the mobile device should enable encryption of device data and any removable data stores. From a usability aspect, it is important that the data encryption does not incur too high of a performance impact, and that data is encrypted in real time and "in place" as opposed to using secure "containers."

Most of today's smartphones include some form of removable media to store documents, photos, music or videos. Instead of using a cable, a user might want to transfer data to and from their personal computer using removable memory, i.e. SD card or USB storage. Some companies will permit the use of removable storage, but others may find this unacceptable because of the regulatory and legal issues surrounding sensitive customer or patient data. If an organization does allow removable media, the data on the removable media should be encrypted as securely as the data stored on the device.

Virus and Other Malware Protection

Downloading and installing mobile applications can increase the productivity of mobile workers. However, this flexibility may also introduce security risks as wireless devices become new targets for malicious third parties seeking to compromise a device or a corporate network. Viruses, Trojans, worms and other malware can be unknowingly loaded onto wireless devices. Malware threatens information confidentiality, endangers system passwords and increases the risk of data loss or compromise. A secure wireless solution should minimize malware risks to corporate networks and devices by preventing malware from being loaded onto the mobile devices and limiting what damage the malware can do if it does happen.

Type of Malware	Description
Virus	Replicates itself by attaching to legitimate applications on a mobile device. Characterized by both its propagation and the delivery method, and actions that it performs might require a trigger to run.
Trojan Horse	Disguises or embeds itself within a seemingly innocuous or trusted application. Depends on the action of the user to succeed, and requires successful use of social engineering rather than the ability to exploit flaws in the security design or configuration of the target.
Worm	Replicates itself to spread across networks. Can potentially overwhelm mobile devices and fixed computer systems, and does not need to be a part of another application in order to spread itself.
Spyware	Designed to log and report user activities and personal data.

The most common approach for preventing the transmission and proliferation of malware on computers is to install virtual, real-time anti-virus scanning software. This software is designed to detect and contain malware. Desktop computers can easily accommodate anti-virus software, but many mobile devices are constrained by memory, processing power and battery life.

Detecting malware requires a large, frequently updated local database or a constant connection to an online database. As a result, the device is constantly downloading new data and running processes. These tasks can have a significant impact on battery life, can increase network traffic and slow other mobile device operations.

Another approach to protect against malware on mobile devices is to proactively prevent mobile devices from downloading or running unauthorized programs or to restrict what features and functions an application can use. Some approaches include:

- Specify exactly which applications — trusted, corporate-approved applications only — are permitted on the device
- Prevent third party applications from using persistent storage on the device
- Determine which resources — such as email, phone, and device encryption key and certificate-store — third party applications can access on the device
- Restrict the types of connections — such as network connections inside the firewall — that a third-party application running on the device can establish
- Block all third party applications from loading onto and running on the device.

Security of Bluetooth Connections on Mobile Devices

Bluetooth® is a standard for short-range wireless technology that enables devices such as laptops, PDAs, smartphones, hands-free car kits or headsets to communicate with each other over a short range (approximately 10m). In the past, Bluetooth has been the subject of high profile security concerns, such as “Blue-jacking.” However, the bigger security issue is often the default factory settings for new Bluetooth devices. Many Bluetooth devices are shipped with security disabled and default to “Always Discoverable.” They may also use short standard PINs such as “0000,” making it easy for malicious users to find and pair with a device and potentially intercept the flow of data. Furthermore, the malicious user may even gain access to core device functionality, such as voice, data and messaging. Devices with Bluetooth can also be targets of Denial of Service (DoS) attacks. DoS attacks typically bombard the device with requests, resulting in an unresponsive device or causing the battery to drain.

To maintain security, each time a user attempts a connection via Bluetooth, the device should alert the user and require confirmation that it is connecting to a trusted device using Bluetooth technology. In addition, all data traffic that is transmitted between these connected wireless devices should be encrypted. This can prevent hackers from connecting and downloading data without user knowledge, as well as “sniffing” traffic as it is being transmitted.

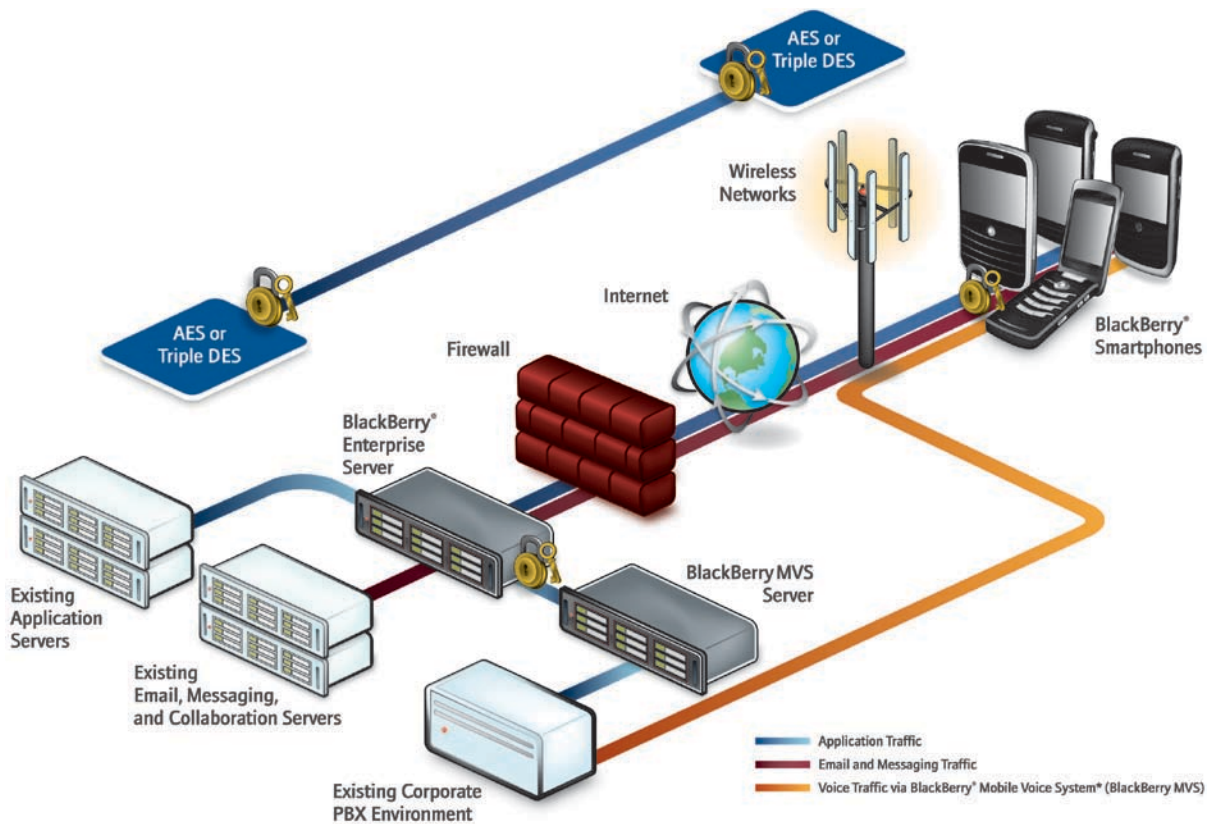
Bluetooth profiles specify how applications on Bluetooth enabled devices connect and interoperate. Wireless security policies are often needed to control which devices can connect using Bluetooth technology and which Bluetooth profiles are available on those devices. Some companies allow Bluetooth headsets for voice but not Bluetooth access for data from laptops or other mobile devices. In other instances, only a subset of employees are allowed to use Bluetooth technology to connect to specific peripheral Bluetooth enabled devices, such as smart card readers, bar code scanners or credit card readers.

Securing the Communications to and from the Mobile Device

These days, data applications such as email, SMS and MMS messaging and web-browsing are responsible for more wireless network traffic than voice. The global growth in 3G networks, public Wi-Fi deployments (Hotspots), and home and business Wi-Fi can provide a reliable, seamless wireless network for these popular data applications. Unfortunately, much of this incredible growth in mobile data usage is not secure. Mobile workers are frequently using unsecured public networks to exchange sensitive corporate email and access strategic business applications, often without any thought to potential consequences. A 2008 online survey found that about 30% of U.S. and Canadian mobile users access the Internet wirelessly, and almost two-thirds of these North American users said that they lack any security software on their mobile devices.

Since most wireless networks being used by mobile workers reside outside of the corporate environment, organizations need to assume that no inherent data protection exists. Everyday, an enterprise's most important information assets can be transmitted over any wireless network, making protection of corporate data in transit

critical. One of the measures by which an organization can assess the strength of a wireless solution's security is through its ability to maintain confidentiality, integrity and authenticity of data throughout its journey across the wireless network, from mobile device to the enterprise network.



* Applicable to BlackBerry MVS for Cisco Unified Communications Manager. BlackBerry MVS requires a media gateway, where voice traffic routes through the BlackBerry MVS server during every inbound and outbound BlackBerry MVS call.

Confidentiality, Integrity and Authentication Over the Network

Administrators need to make sure that the connection over the wireless network is highly secure, to maintain data confidentiality and integrity, and to authenticate the origin of the data. Confidentiality refers to the process of preventing access to information by anyone other than the intended recipient. Integrity enables a recipient to detect whether a message has been modified by a third party while in transit, and authentication allows the recipient to identify the sender and trust that this sender actually sent the message. Strong data confidentiality and integrity are especially critical for wireless traffic, as data can be more easily intercepted - and potentially compromised - by virtually anyone in vicinity of the wireless network.

Confidentiality

Two common ways in which a wireless solution can provide data confidentiality are through data encryption and the use of an encrypted tunnel over which the data is transmitted. Data encryption uses a secret key to encode information in a manner that can only be decoded and read by the parties for which it is intended. Most modern cryptography solutions are based on the Advanced Encryption Standard (AES). AES is required by U.S. government agencies and is considered secure enough to be used in sensitive military applications. An encrypted tunnel is setup when a Hypertext Transfer Protocol (HTTP) connection is established over Secure Socket Layer/Transport Layer Security (SSL/TLS). This provides additional authentication and security if wireless devices are accessing servers on the Internet. Many secure internet transactions, such as online banking, require support for Hypertext Transfer Protocol Secure (HTTPS).

Authentication

Authenticity allows the recipient to identify the sender and trust that the sender actually sent the message. To prevent unauthorized users from pretending to be a legitimate device and accessing the network, a device should authenticate itself to the network and enterprise systems. Conversely, the server should authenticate itself to the mobile device to prevent unauthorized users from pretending to be a corporate server. Authentication can be accomplished through the use of a

cryptographic shared key system. A shared key system requires that an authenticating component (such as a server) and a requesting component (such as a wireless device) both know a secret key. When a connection is attempted, the server sends the secret key, and the wireless device either accepts or rejects the key. Before encrypting the data to be transmitted, the wireless device checks with the back-end system to determine if the keys match. For successful data transmission to occur, the keys on the server and the wireless device must match. If the keys do not match, the server and the wireless device cannot send data between them.

Integrity

Data integrity refers to the validity of the transmitted data (i.e. whether the data has undergone changes or modification in transit). The trustworthiness of data can be determined using various prevention and detection mechanisms. With encrypted data, message failure will occur automatically if the message format is unrecognized in the decryption process. Failure will also occur if the message received is encrypted using the wrong encryption key or if the encrypted data has been changed during transit. The wireless solution under consideration should automatically eliminate changed packets of data to ensure that malicious or false data has not replaced the valid data.

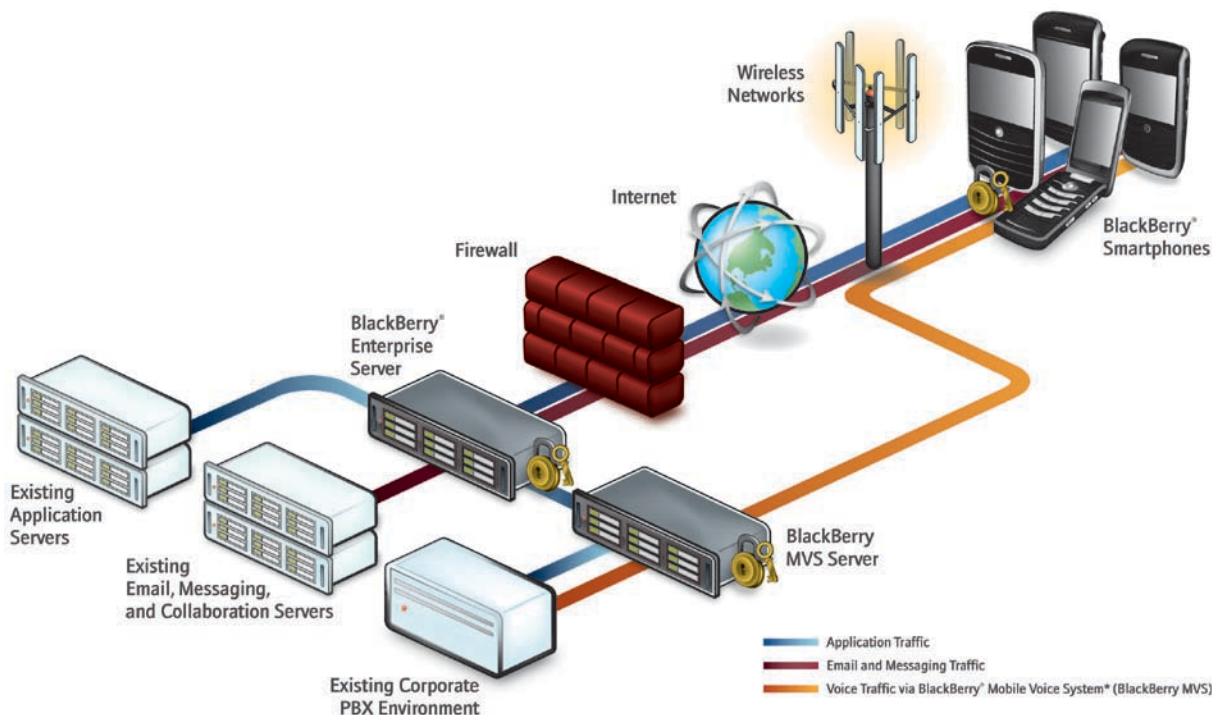
Optimizing the Enterprise Network to Support Business Mobility

The growth of Business Mobility is forcing organizations to rethink their network architecture and the scope of perimeter security. In the old days of the desktop computers and wired networks, organizations relied on firewalls, VPNs and hardware authentication to protect their network from unauthorized external access. Perimeter security was provided by a device, such as a firewall, that inspected packets and sessions to determine if they should be transmitted to or from the protected network. In addition, networks were often segmented using VLANs and subnets to improve security and mitigate risk.

Extending the Network Perimeter to the Mobile Worker

With the rapid growth in mobile computing, companies are forced to extend their definition of the network perimeter to include mobile devices and their wireless connections to the network. Since mobile devices are often used outside the firewall, administrators need to secure firewall port openings and inbound- and outbound-initiated connections to ensure that only authorized IP addresses are communicating on authorized ports. In the inbound connection model, the source is not known in advance of any connection attempt and is therefore not trusted, requiring that controls be implemented to mitigate the inherent risks involved.

With outbound-initiated connections, the source and destination port numbers and the IP addresses are known to the corporate network. The IT department can implement appropriately detailed internal controls on those ports to secure outbound connections. When changing firewall configurations to accommodate a wireless solution, permitting only outbound-initiated connections can reduce the risk of unauthorized access, compared to use of an inbound-initiated connection. “Pushing” information to the mobile device is inherently more secure than “Pulling” it, since the destination is known and there is reduced likelihood of the data being intercepted. Pushing is also easier on device resources such as battery power, as the mobile device no longer has to “poll” the remote system to determine if information is ready for download.



* Applicable to BlackBerry MVS for Cisco Unified Communications Manager. BlackBerry MVS requires a media gateway, where voice traffic routes through the BlackBerry MVS server during every inbound and outbound BlackBerry MVS call.

Segmenting the Network for Security and Reliability

To improve the Quality of Service (QoS) and prevent the spread of malware on your organization's network, you can divide your organization's network or LAN into multiple segments, all separated by firewalls, to create a segmented network architecture. Each network segment can contain application-specific network traffic, designed to improve the security and performance of the network by filtering out data that is not destined for that specific segment. The corporate firewall is still a critical component to protecting the organization's network from attack. Since mobile devices are used outside the firewall, administrators need to secure firewall port openings and inbound- and outbound-initiated connections to ensure that only authorized users with known IP addresses are communicating on authorized ports.

Device Management makes it Easy

To ease the burden and cost, IT administrators need the ability to automatically establish, enforce and update mobile device settings. Policy administration should be centralized to provide comprehensive control across all classes and types of mobile devices and mobile operating systems. IT administrators should be able to deploy group policies to reflect the needs of various teams and users within the organization. After an IT administrator sets a mobile device policy, users should not be able to intervene or prevent the policy from being applied.

Users should be encouraged to report lost or stolen devices as soon as possible. Automated policies, procedures and technologies should be put in place to deactivate any lost or stolen device to prevent unauthorized access from potentially compromised terminals. The administrator should also have the ability to audit the successful application of the wireless security policy on the mobile device.

Conclusion

As Business Mobility continues to mature and the use of mobile devices in enterprise reaches critical mass, organizations need to take the necessary steps to maintain the security of their sensitive data. The portable nature of the mobile device means that corporate data is increasingly transmitted outside the corporate network and stored on mobile devices outside the physical boundaries of the organization. While losing data is only an embarrassment for some organizations, financial and legal risks may result in many cases. The most effective way to maintain corporate data security while accommodating the increase in Business Mobility is through a comprehensive wireless security strategy.

The most effective wireless security strategy is a proactive one: to develop, educate, enforce and maintain an enterprise-wide wireless security policy. An effective wireless security solution should be an extension of the standard enterprise security mandate, but engineered specifically for the realities of mobility. In many cases, solutions that work in a desktop environment are impractical for mobile computing, given the constrained processing, memory

and battery resources of mobile devices. To be effective, an enterprise wireless security strategy needs to address:

- Securing the mobile device and its data
- Securing the communications to and from the mobile device to the corporate network
- Optimizing the enterprise network to support Business Mobility.

For More Information

RIM offers a number of different resources to learn more about wireless solutions in general and BlackBerry in particular.

The website www.blackberry.com is a good place to start. The Technical Knowledge Center on the site at www.blackberry.com/support can help you get answers to specific questions. To find other CIO Guides, including The CIO's Guide to Wireless, The CIO's Guide to Mobile Applications, The CIO's Guide to Fixed Mobile Convergence and more, visit www.blackberry.com/getthefacts

Related Resources

To learn about how the BlackBerry® Enterprise Solution is designed to help organizations develop, plan and implement their mobile security initiatives, visit www.blackberry.com/security

Resource	Information
BlackBerry Enterprise Solution Security Technical Overview	<ul style="list-style-type: none"> • Describes the security features of the BlackBerry Enterprise Solution • Provides an overview of the BlackBerry security architecture.
BlackBerry Enterprise Solution Security Acronym Glossary	<ul style="list-style-type: none"> • Full terms substituted by acronyms in this and other security documents.
BlackBerry Signing Authority Tool Administrator Guide	<ul style="list-style-type: none"> • The BlackBerry Signing Authority Tool implementation of public key cryptography.
BlackBerry® Smart Card Reader Security Technical Overview	<ul style="list-style-type: none"> • Highly secure pairing between the BlackBerry® smartphone and the BlackBerry Smart Card Reader • Initial key establishment protocol • Connection key establishment protocol.
Policy Reference Guide	<ul style="list-style-type: none"> • Using BlackBerry Enterprise Server IT policies.
Security for BlackBerry Smartphones with Bluetooth Wireless Technology	<ul style="list-style-type: none"> • Bluetooth wireless technology overview • Using and protecting Bluetooth enabled BlackBerry smartphones • Risks of using Bluetooth wireless technology on mobile devices.
Placing the BlackBerry Enterprise Solution in a Segmented Network	<ul style="list-style-type: none"> • Components in a segmented network • BlackBerry Enterprise Solution connection types and port numbers overview • Changing port numbers.
Protecting the BlackBerry Smartphones Platform Against Malware	<ul style="list-style-type: none"> • Managing the risks of malware attacks • Using BlackBerry Enterprise Solution tools to contain malware on BlackBerry smartphones.
Enforcing Encryption of Internal and External File Systems on BlackBerry Devices Technical Overview	<ul style="list-style-type: none"> • System requirements and IT Policy requirements for file encryption on BlackBerry smartphones • Protecting user data stored on locked BlackBerry smartphones • Protecting files stored in external memory on BlackBerry smartphones.

Appendix A - Mobile Security Checklists

Securing the Mobile Device and its Data

- Label all mobile devices with user and company information.
- Require a user to authenticate to the device using a security password.
- Define authentication features, such as password expiry, attempt limits, length and strength.
- Ensure that all devices have timeout mechanisms that automatically prompt the user for a password after a period of inactivity.
- Prevent mobile devices from downloading untrusted third-party applications over the wireless network.
- Regularly backup all data on the device.
- Keep the software and settings on the device up to date. (OS patches, anti-virus signatures, firewall settings, etc.)
- Follow guidelines for safe synchronization and include password authentication.
- Specify whether or not applications, including third-party applications, on the mobile device can initiate specific types of connections.
- Enforce security and policy controls through an IT managed server

Securing Communications to and From the Mobile Device

- Uses encryption to protect data in transit (i.e., AES-256, AES-192, AES-128, Triple DES, etc.) and at rest.
- All wireless communication should, if possible, use strong cryptography, have robust key management and have strong user authentication.
- Wireless devices must maintain a hardware address that can be registered and tracked (i.e., a MAC address).
- Disable Bluetooth functionality when not in use.
- Restrict automatic connections on mobile devices. Always prompt for a connection.
- Install VPN software on all mobile devices.
- Mobile devices should include personal firewall and anti-virus software with automatic updates.
- Do not allow wireless clients to engage in ad-hoc communications (i.e., connect to other, unknown wireless devices directly).
- Mobile devices should include interface blocking utilities (i.e., the ability to turn on or off SMS, MMS or Bluetooth capabilities).
- Forced management through IT push (through a server).



This material, including all material incorporated by reference herein or made available by hyperlink, is provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation or warranty of any kind by Research In Motion Limited and its affiliated companies ("RIM") and RIM assumes no responsibility for any typographical, technical, or other inaccuracies, errors or omissions in this material and shall not be liable for any type of damages related to this material or its use, or performance, or non-performance of any software, hardware, service, or any references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party web sites (collectively the "Third Party Products and Services"). RIM makes no representation, warranty or guarantee and assumes no liability whatsoever in relation to Third Party Products or Services.

The limitations and exclusions herein shall apply irrespective of the nature of the cause of action and in no event shall any director, employee, agent, distributor, supplier or independent contractor of RIM have any liability related to or use of the material.

© 2010 Research In Motion Limited. All rights reserved. BlackBerry®, RIM®, Research In Motion®, SureType®, SurePress™ 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. PGP is a trademark of PGP Corporation. Wi-Fi is a trademark of the Wi-Fi Alliance. All other trademarks are the property of their respective owners. MKT-31415-001