The CIO's Guide to Mobile Security

Executive Overview and Checklist

The CIO's Guide to Mobile Security

Table of Contents

Executive Summary

Today’s enterprise and government organizations increasingly support the use of mobile (wireless) devices by their employees. Executives, managers, contractors, suppliers and other corporate employees are connecting their wireless devices to corporate email servers: sales teams need access to customer and order information held within their company CRM systems; field technicians need to receive and interact with service information; and managers require timely access to critical business data from their business intelligence system. Across organizations, users seek to improve their productivity through the access of corporate data from mobile devices.

At the same time, enterprise and government organizations often underestimate the potential security risks of using wireless devices. Organizations need to approach securing wireless devices in the same way that they approach securing the wired components of the corporate local area network (LAN), such as servers, desktop computers and laptop computers. Organizations can establish an overall infrastructure for security that includes wireless devices by installing security features on the devices and implementing appropriate security policies. While implementing security solutions is critical, the unique challenge facing those tasked with wireless security is the direct impact of security measures on the user experience. Creating a secure environment on a mobile device often requires additional device processing power, storage, and battery life. This means that, as a mobile device becomes more secure, it places greater strain on its resources, which affects the performance of the device.

This document examines six key mobile computing security concerns that an IT department should consider when evaluating a wireless solution.

Minimizing mobile computing security vulnerabilities

Wireless solution security addresses the need to secure data transmission through encryption, authentication, authorization, access control and firewall protection down to the wireless device level. As wireless solutions continue to build momentum and the subsequent number of wireless devices grows, the demand to manage and secure these solutions increases.

Most organizations do not allow remote employees with laptop computers to connect to business systems behind the corporate firewall without the use of a virtual private network (VPN) connection. However, many wireless devices often operate in this manner by default—accessing corporate assets with little or no security.

Wireless devices have rapidly evolved past cellular phones and “dumb” client PDAs. Today, many devices are designed to interact with corporate assets in a client-server architecture. This presents IT administrators with the challenge of securing a client that resides outside the corporate network and accesses sensitive data that lies within that network. When wireless devices access corporate data, security vulnerabilities can arise in the following six main areas—each of which should be considered when evaluating a wireless security solution:

1. Integrity of the corporate firewall

Corporate firewalls are critical components for protecting an organization’s network from attack. Since mobile devices are used outside the firewall, administrators need to secure the firewall port openings and ensure that changes in the firewall configuration to accommodate mobile device connections do not impact the organization’s existing security policies.

2. Confidentiality, integrity, and authenticity over the network

Administrators need to make sure that the connection over the wireless network is secure to maintain data confidentiality and integrity, and to authenticate the origin of the data. An email message or any other type of data is considered to be confidential if only the intended recipient can view the contents of the message. Integrity enables a recipient to detect whether a message has been modified by a third party while in transit. Authenticity allows the recipient to identify the sender and trust that the sender actually sent the message.

3. Confidentiality of data on the devices

Mobile devices are more likely to be subject to loss, theft, and tampering than other corporate IT resources as they are designed to be used outside an organization's physical confines. All data on the mobile device and any removable memory should be encrypted to protect user data on the device against third-party access if the device is stolen.

4. Virus and other malware protection

Mobile devices can increase the productivity of mobile workers. However, this flexibility introduces security risks as wireless devices become new targets for malicious third parties seeking to compromise a device or a corporate network. If viruses, trojans, worms, and other malware are loaded onto wireless devices, they might run on the devices without the user's knowledge or action. A wireless solution should minimize malware risks to corporate networks and devices by preventing malware from being loaded onto the mobile devices and limiting what the malware can do if this occurs.

5. Support existing corporate security standards

Most IT departments have already established corporate security standards. Wireless deployments should not sacrifice any existing policies; instead, the solution should support these standards in order to extend corporate security to the wireless devices.

6. Establish, enforce, and periodically update security policies

Effective mobile security includes the ability to mandate passwords for users, erase data from devices remotely, and lock the device remotely. Administrators also need the ability to establish, enforce and update settings through policies or parameters, as well as provide comprehensive control across all devices.

Integrity of the corporate firewall

The corporate firewall is a critical component that helps to protect an 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 IP addresses are communicating on authorized ports.

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.

Inbound-initiated firewall connections

Administrators rely on firewalls to control access to corporate network resources. An inbound-initiated connection opens a firewall port, allowing a connection into corporate assets from non-corporate access points such as wireless devices, shared computers, or public Internet kiosks. In the inbound connection model, the source is not known in advance of any connection attempt, and therefore is untrusted, requiring that controls be implemented to mitigate the inherent risks involved.

External users, including users with mobile devices, initiate inbound connections to the corporate network. Many companies choose to maintain control over the device connections by using a client-authenticated SSL connection, which is designed to mitigate the risk of an inbound connection to the corporate network. For wireless solutions that permit inbound-initiated firewall connections, increasing firewall connection limit time-outs beyond what would normally be considered acceptable and secure is recommended. This approach provides users with the opportunity to receive email messages and other data as close to real-time as possible, while preserving the scarce battery resources on the device (each time the connection is lost and re-established, the battery is depleted). However, increasing the connection limit time-outs can increase the risk of unauthorized access to your internal networks, increasing the risk of a security breach on the corporate network.

Outbound-initiated firewall connections

With an outbound-initiated connection, software behind a firewall typically contacts the Network Operations Center (NOC) which facilitates connections with each of the wireless networks that are available to the mobile device users. As the connection is initiated from within the corporate network perimeter, users are aware of both the source and destination of the connection. They may then configure the firewall with both of those items and the specific port for the connection.

When connecting to a third-party NOC through the outbound firewall connection, a secure solution uses a security handshake to establish the credentials and authorize the connection: if authentication fails then the connection is not established. However, once the connection is authorized and established, it remains a persistent session for communication with the authorized wireless device through the NOC only. The firewall immediately discards any other inbound traffic from another host. Since the firewall does not respond to any inbound-initiated connections, it does not respond to malicious incoming packets.

Using a NOC to boost firewall integrity provides several benefits. A NOC solution enables enterprises to offload responsibility for managing outbound-initiated connections with mobile operators. Companies are also able to use a variety of operators or move to new ones without changing their wireless technology. A NOC-based architecture can also improve security as it does not require organizations to open inbound ports in their firewalls. In addition, a NOC provides an alternate means for teams to communicate if their home-based telecom systems fail.

Confidentiality, authenticity, and integrity over the corporate network

Since the wireless network resides outside of the corporate environment, organizations need to assume that no inherent data protection exists. An enterprise's most important information assets can be transmitted over the 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.

Confidentiality of data in transit

Confidentiality refers to the process of preventing access to information by anyone other than the intended recipient. Two common ways that a wireless solution provides data confidentiality are through data encryption and the use of an encrypted tunnel over which the data is transmitted.

Data encryption is data scrambling based on a secret key. To decrypt and read the encrypted data, access to the secret key is required. Two of the strongest data encryption standards in use today are Advanced Encryption Standard (AES) and Triple Data Encryption Standard (Triple DES); both are industry standard algorithms and well used throughout government and financial industries. AES is considered the most resource-conservative approach and the encryption method of choice for the US government as well as other security-conscious governments and organizations worldwide.

An encrypted tunnel is generally established using the SSL protocol. This is an acceptable level of data protection for most organizations and is used in many online applications, including Internet banking.

However, using an SSL-protected connection requires an inbound firewall connection, and in order to achieve a "push-like" experience where information is sent in as close to real-time as possible, the connection must be constantly removed and rebuilt. This can be very resource-intensive and tends to negatively affect the battery life of mobile devices.

Data authenticity

Authenticity allows the recipient to identify the sender and trust that the sender actually sent the message. In order to prevent unauthorized users from pretending to be a legitimate device, the device should authenticate itself to the network and enterprise systems. Similarly, the enterprise server should authenticate itself to the device to prevent unauthorized users from pretending to be the 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) 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.

Data integrity

Data integrity refers to the validity of the 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. Likewise, 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.

Confidentiality of Data on the Devices

Company information stored on a mobile device should be just as secure as information stored on a corporate network. Some companies suffer only embarrassment from incidents in which corporate data is accessed by unauthorized parties. Unauthorized access of devices can also result in problems such as identity theft or industrial espionage. For public companies and 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 doctors and health care companies, the loss of patient data compromises patient confidentiality, which is protected by the Health Insurance Portability and Accountability Act (HIPAA).

Data stored on mobile devices can be secured by controlling access to the device itself in several ways. These include using passwords and/or two-factor user authentication mechanisms, encrypting the data stored on the device and on removable media, and securing non-physical access to the device, such as through Bluetooth® technology.

User authentication

Device information is protected in several ways; the most common is user authentication through the use of an individual password. The objective of the password is to ensure that only the 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 multi-factor authentication through the use of smart cards or other, similar mechanisms. Two-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" that is unique to the user (for example, the user's fingerprint).

Security of stored data on mobile devices

According to the Gartner Group, over 250,000 PDAs were lost in 2001 alone. The loss of wireless devices presents numerous potential threats, including unauthorized access to:

- device data and functionality
- corporate servers and applications

Many wireless solutions today provide the ability to remotely erase the data from the device. However, a time lag often exists between when a user loses the device and when the user contacts the IT department to report the device missing. An unauthorized user could access the device and extract the data during this time lag. To prevent this, a wireless solution should enable real-time encryption of device data.

Security of removable data on wireless devices

When data is stored on a mobile device, users might want to transfer that data to a non-corporate device via removable memory. For some companies, this is perfectly acceptable, assuming that employees will use discretion in sharing data with other individuals. For other organizations—typically government, legal, health care, pharmaceutical, and financial institutions—this is not acceptable due to the legal issues surrounding sensitive corporate data. In addition, because removable memory can present an opportunity to inadvertently introduce a virus to the device and the corporate network, organizations sometimes restrict its use.

If an organization allows removable media, a wireless solution should provide the option for encrypting the data and establishing wireless security policies that define groups of users that are permitted to use this type of media.

Security of Bluetooth connections on mobile devices

Bluetooth is a wireless technology that allows Bluetooth-enabled devices to establish a wireless connection with other Bluetooth-enabled devices that are within a specified range. 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 prevents hackers from connecting and downloading data without user knowledge, as well as "sniffing" traffic as it is being transmitted.

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. In addition, cell phone worms such as Cabir can use Bluetooth technology to propagate.

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.

Virus and other malware protection

Like their attacks and proliferations on desktops and laptops, viruses, Trojans, worms, and spyware—collectively referred to as malware—can load themselves onto wireless devices and run without user knowledge or action. The successful installation and operation of a simple malware program can effectively use all available memory and halt device performance. A more dangerous malicious program can transmit itself across the wireless network, bypassing some of the corporate network security systems, and potentially damaging other components of the corporate network.

Protecting against malware

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.

While desktop computers easily accommodate anti-virus software, wireless 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, increase network traffic and slow other device operations.

One approach to protect against malware on mobile devices is to proactively prevent mobile devices from loading or running unauthorized code. This tactic is designed to give system administrators the ability to perform the following actions:

- 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 certificatestore—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

Attachment viewing and malware

Email attachments that users open on wireless devices can contain viruses and other malware. Proactive solutions using an attachment service employ renditions rather than supporting native files. In this scenario, the user can still view and manipulate the data, but the file is not opened natively on the device. This measure is designed to prevent malicious applications from accessing data on the device.

If a wireless solution includes a remote, protected server to perform attachment-related actions, the attachment-processing server can still be vulnerable to attack from viruses and other malware. However, it is easier for the IT department to install software on this server rather than on the mobile device to help prevent these attacks, and the server is not constrained by processing power or battery life. If it is required, the attachment-processing server can be isolated from the corporate network since it resides within the corporate infrastructure.

Support existing corporate security standards

Most IT organizations have already established corporate security standards, and the wireless solution should support these standards. Table 1 lists some of the more common security standards in place today and how these can be integrated into a wireless solution.

Security Standards	Wireless Use
Smart Card Readers	Smart cards can be used for two-factor authentication, secure messaging, and secure web browsing.
RSA SecurID Support	There are two types of RSA SecurID support currently available: 1. Users can access an application on the wireless device that generates token numbers and then use their laptop and VPN to access corporate systems. 2. The wireless device communicates with the RSA corporate servers to secure a connection before transmitting data. For example, when a user navigates to a site or application on the wireless device requiring authorization, the device prompts the user for their username and token passcode.
Sender-to-Recipient Encryption Support	Standards such as S/MIME, PGP and Lotus Notes native encryption enable sender-to-recipient confidentiality, integrity, and authentication.
HTTPS, SSL/TLS	A Hypertext Transfer Protocol (HTTP) connection can be established over Secure Socket Layer/ Transport Layer Security (SSL/TLS) to provide 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).
WTLS	Wireless Transport Layer Security (WTLS) is designed to provide an extra layer of security when connecting to a Wireless Application Protocol (WAP) gateway. WTLS requires a WAP gateway to provide standard WAP access to the Internet. To use a WAP gateway, a company must work with the network operator or service provider.

Establish, enforce and periodically update security policies

IT administrator-controlled security policies

Most organizations implement appropriate security measures to ensure that only authorized devices (wired or wireless) are connected to the network. These measures include standard policies that address user authentication, network security and virus protection.

When extending the organization's security policies to mobile devices, 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.

In the early years of mobile data access, first-generation wireless security policies were broad and covered a wide range of concerns, including privacy and appropriate use of the device. Typically, a single policy addressed multiple concerns. However, as mobile access to information becomes more prevalent and organizations become more mobility-dependent, a limited series of broad IT policies can no longer meet the needs of most organizations. Conversely, a robust set of security policies provides granular control over all aspects of the wireless solution.

The following example policies define acceptable security and functionality for corporate mobile devices.

1. Define acceptable user authentication:
   - require a user to authenticate to the device using a security password;
   - configure features such as password expiry, attempt limits, length, and strength;
   - require and define acceptable corporate passwords and pass phrases on mobile devices in your organization
2. Define measures to protect mobile devices from unauthorized use:
   - restrict connections permitted on mobile devices;
   - use encryption of data in transit between the sender and recipient of wireless data;
   - encrypt removable media used with mobile devices;
   - encrypt data stored on mobile devices
3. Define acceptable encryption of mobile device data:
   - require a specific standard of encryption strength
4. Define virus and malicious user prevention measures:
   - prevent mobile devices from downloading third-party applications over the wireless network;
   - specify whether or not applications, including third-party applications, on the mobile device can initiate specific types of connections

IT administrators should be able to deploy group policies to reflect the needs of various teams and users within the organization. All policy settings should be synchronized and assigned to the device using a wireless connection.

After an IT administrator sets a mobile device policy, users should not be able to intervene or prevent the policy from being applied. The administrator should also have the ability to audit the successful application of the wireless security policy on the mobile device.

Example security checklist

The checklist below provides a list of key issues to consider when evaluating the security of wireless solutions. The “Included” column can be used to indicate that the functionality is available in the solution, and the “Add-on” column indicates whether or not additional components must be purchased to gain the required functionality.

Wireless Solution Functionalities	Wireless Solution Option A		Wireless Solution Option B	
	Included	Add-on	Included	Add-on
Wireless Data Security				
Uses encryption to protect data in transit (i.e. AES-256, AES-192, AES-128, Triple DES etc.)				
Uses an Outbound Connection for Server Authentication				
Ability to Disable Bluetooth				
Ability to Disable SMS and MMS Messages				
IBM® Lotus Notes® Email Encryption Support				
Device Data Security				
Virtual Real-Time Encryption of Device Data				
Optional Data Shredding on Device Wipe				
Ability to Disable Attachment Viewing				
Ability to Force Encryption of Data on External Storage Cards				

Wireless Solution Functionalities	Wireless Solution Option A		Wireless Solution Option B	
	Included	Add-on	Included	Add-on
User Authentication				
Ability to Force password Authentication on Device				
Ability to Enforce Strong Device Passwords				
Ability to Enforce a Forbidden Password List				
Ability to Force Device to Lock After a Certain Amount of Time of Inactivity				
Remote Control				
Ability to Remotely Change the Device Password				
Ability to Remotely Wipe the Device				
Application Control				
Ability to Force the Installation of Important Applications				
Ability to Disable the Downloading of all Third-Party Applications				
Ability to Disable a Specific Application on all Devices				
Increased Security Options				
S/MIME Encryption Support				
PGP Encryption Support				
Support for Two-Factor Authentication				

Summary

As the use of mobile devices in enterprise organizations increases, corporate and government organizations need to take the necessary steps to maintain the security of their email and application data. In using wireless devices, data is increasingly transmitted outside the corporate network and stored on mobile devices outside the physical boundaries of the organization. Mobile devices are potentially subject to man-in-the middle attacks, DoS attacks, malware threats, and other data breaches. While losing data is only an embarrassment for some organizations, financial and legal risks may result in many cases.

An effective wireless solution should be designed for enterprise-grade security and provide an architecture 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. The corporate firewall is a critical component in protecting an organization's data and should protect against opportunities for attack or malicious use. The connection over the wireless network must be secure to maintain confidentiality, authenticity, and integrity of the data transmitted. And finally, mobile devices must be protected from data loss, tampering and malware infection.

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 www.blackberry.com/go/getthefacts

Resource	Information
BlackBerry Enterprise Solution Security	• Describes the security features of the BlackBerry Enterprise Solution • Provides an over of the BlackBerry® security architecture
BlackBerry Enterprise Solution Security Acronym Glossary	• Full terms substituted by acronyms in this and other security documents
BlackBerry Signing Authority Tool Administrator Guide	• The BlackBerry Signing Authority Tool implementation of public key cryptography
BlackBerry Smart Card Reader Security White Paper	• Secure pairing between the BlackBerry device and the BlackBerry® Smart Card Reader • Initial key establishment protocol • Connection key establishment protocol
Policy Reference Guide	• Using BlackBerry Enterprise Server IT policies
PGP Support Package White Paper	• PGP security and encryption • Using PGP Universal Server to store and manage PGP keys • Searching for and validating PGP keys • Sending and receiving PGP messages
PGP Support Package User Guide Supplement	• Installing the PGP Support Package • Managing PGP keys on the BlackBerry device • Setting PGP options for digitally signing and encrypting messages
S/MIME Support Package White Paper	• S/MIME security and encryption • Managing S/MIME certificates on the BlackBerry device and desktop computer
S/MIME Support Package User Guide Supplement	• Installing the S/MIME Support Package • Managing certificates on the BlackBerry device and desktop computer • Setting S/MIME options for digitally signing and encrypting messages • Sending and receiving S/MIME messages
Security for BlackBerry Devices with Bluetooth Wireless Technology	• Bluetooth wireless technology overview • Using and protecting Bluetooth-enabled BlackBerry devices • Risks of using Bluetooth wireless technology on mobile devices
BlackBerry Wireless Enterprise Activation Technical Overview	• Wireless enterprise activation process • Wireless master encryption key generation • Initial key establishment protocol • Key rollover protocol
Wireless LAN Security	• Security options for implementing a supported BlackBerry device on a WLAN

*Check with service provider for availability, roaming arrangements and service plans. Certain features outlined in this document require a minimum version of BlackBerry Enterprise Server software, BlackBerry Desktop Software, and/or BlackBerry Device Software. May require additional application development. Prior to subscribing to or implementing any third party products or services, it is your responsibility to ensure that the airtime service provider you are working with has agreed to support all of the features of the third party products and services. Installation and use of third party products and services with RIM’s products and services may require one or more patent, trademark or copyright licenses in order to avoid infringement of the intellectual property rights of others. You are solely responsible for determining whether such third party licenses are required and are responsible for acquiring any such licenses. To the extent that such intellectual property licenses may be required, RIM expressly recommends that you do not install or use these products and services until all such applicable licenses have been acquired by you or on your behalf. Your use of third party software shall be governed by and subject to you agreeing to the terms of separate software licenses, if any, for those products or services. Any third party products or services that are provided with RIM’s products and services are provided “as is”. RIM makes no representation, warranty or guarantee whatsoever in relation to the third party products and services and RIM assumes no liability whatsoever in relation to the third party products and services even if RIM has been advised of the possibility of such damages or can anticipate such damages.

The handheld and/or associated software are protected by copyright, international treaties and various patents, including one or more of the following U.S. patents: 6,278,442; 6,271,605; 6,219,694; 6,075,470; 6,073,318; D,445,428; D,433,460; D,416,256. Other patents are registered or pending in various countries around the world. Please visit www.rim.net/patents.shtml for a current listing of applicable patents.

This document is provided “as is” and Research In Motion Limited (RIM) assumes no responsibility for any typographical, technical or other inaccuracies in this document. RIM reserves the right to periodically change information that is contained in this document; however, RIM makes no commitment to provide any such changes, updates, enhancements or other additions to this document to you in a timely manner or at all. RIM MAKES NO REPRESENTATIONS, WARRANTIES, CONDITIONS OR COVENANTS, EITHER EXPRESS OR IMPLIED (INCLUDING WITHOUT LIMITATION, ANY EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS OF FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, MERCHANTABILITY, DURABILITY, TITLE, OR RELATED TO THE PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE REFERENCED HEREIN OR PERFORMANCE OF ANY SERVICES REFERENCED HEREIN). IN CONNECTION WITH YOUR USE OF THIS DOCUMENTATION, NEITHER RIM NOR ITS AFFILIATED COMPANIES AND THEIR RESPECTIVE DIRECTORS, OFFICERS, EMPLOYEES OR CONSULTANTS SHALL BE LIABLE TO YOU FOR ANY DAMAGES WHATSOEVER BE THEY DIRECT, ECONOMIC, COMMERCIAL, SPECIAL, CONSEQUENTIAL, INCIDENTAL, EXEMPLARY OR INDIRECT DAMAGES, EVEN IF RIM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, INCLUDING WITHOUT LIMITATION, LOSS OF BUSINESS REVENUE OR EARNINGS, LOST DATA, DAMAGES CAUSED BY DELAYS, LOST PROFITS, OR A FAILURE TO REALIZE EXPECTED SAVINGS.

This document might contain references to third party sources of information and/or third party web sites (“Third-Party Information”). RIM does not control, and is not responsible for, any Third-Party Information, including, without limitation the content, accuracy, copyright compliance, legality, decency, links, or any other aspect of Third-Party Information. The inclusion of Third-Party Information in this document does not imply endorsement by RIM of the third party in any way. Any dealings with third parties, including, without limitation, compliance with applicable licenses and terms and conditions, are solely between you and the third party. RIM shall not be responsible or liable for any part of such dealings.