THE DEFINITIVE GUIDE TO ENTERPRISE MOBILE SECURITY

Strategies and Tactics for Business and IT Decision-Makers

BlackBerry®

The Definitive Guide to Enterprise Mobile Security.

Published by BlackBerry Ltd. 2200 University Ave. E Waterloo, ON, Canada N2K 0A7

To download PDF or e-book copies of The Definitive Guide to Enterprise Mobile Security, visit www.blackberry.com/BES12

Copyright © 2015 BlackBerry Ltd. All rights reserved.

BlackBerry and the BlackBerry logo are trademarks of BlackBerry, Ltd. or its subsidiaries. ® indicates registration in the United States. All other trademarks are the property of their respective owners.

U.S. Library of Congress Cataloging-in-Publication Data

BlackBerry Ltd. The Definitive Guide to Enterprise Mobile Security.

Edited by Jaikumar Vijayan, Alex Manea and Eric Lai.

p.cm.

ISBN 978-1-63315-080-5

1. Mobile Security. 2. Enterprise Mobility. 3. Information Technology. 4. Mobile Applications.

U.S. Library of Congress Class and Year: TK5103.2 .H84 2015
Library of Congress Control Number: 2015904706

Except as permitted under the United States Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher.

Thanks to:
Project manager: Jill Thater
Copy editors: Kara Yi, Matt Young
Designers: The PD Group – www.thepdgroup.com

Executive Sponsors: Heidi Davidson, David Kleidermacher, Mark Wilson, and Trace Cohen

Read Blogs.BlackBerry.com, and follow us at Twitter (@BlackBerry4Biz), LinkedIn.com/Company/BlackBerry and SlideShare.net/BlackBerry

7 Foreword:
Enterprises Lag at Mobile Security, Growing Their Risk Profile Every Day

John S. Chen
CEO and Executive Chairman, BlackBerry Ltd.

Chapter 1
Mobile Evolution

8 An Enterprise Mobility Journey
9 New Era of Productivity
11 The Disruptive Power of Mobile Innovation
12 With Change Come Challenges
13 An Organic Evolution
14 Maturing Technologies and Strategies
16 Bancolombia Case Study

Chapter 2
Enterprise Mobility in Regulated Sectors

20 High Stakes, High Security
21 Three Key Questions to Ask About Compliance
22 Data Integrity in the Mobile Enterprise
24 The Anytime, Anywhere Challenge
25 Cost and Risk
27 Device, Content and Communication Security
30 Australian Audit National Office Case Study

Chapter 3

Mobile Risk and Loss

33 The Mobile Threat Landscape
35 Data Loss and Data Leakage
36 Insecure Applications
37 Other Threats
38 Enormous Implications for Regulated Firms
40 Organizations and Mobility Risk
43 Are You Fighting the Right Fight?
44 Rocky Mountain Human Services Case Study

Chapter 4

Managing Mobile Risk in Regulated Sectors

46 As BYOD Limitations Surface, a Look at Other Enterprise Mobility Models
48 Exercises in Futility
49 The Search for Options
50 Choose Your Own Device
52 Corporate-Owned, Personally-Enabled
53 Corporate-Owned, Business-Only
54 Criteria for Choosing Your MDM or EMM Provider
56 Global Insurance Provider Case Study

Chapter 5

Developing an Enterprise Mobility Management (EMM) Strategy

58 Developing a Strategy To Manage Your Mobile Environment
59 Only the Means to an End
60 The Technology Component
63 The Vendor Maze
64 Samuel, Son & Co. Case Study

Chapter 6

Extreme Mobile Device Management

66 Risk Mitigation Via Device Level Controls
67 Password and Authentication Controls
68 Local Encryption
69 Remote Locate and Remote Lock
70 Containerization
71 Over-The-Air Programming and Configuration
72 Additional Controls
74 Unipresalud Case Study

Chapter 7

Extreme Mobile Application & Content Management

76 Securing Mobile Apps and Content for Use in Regulated Sectors
77 Usage Policies
78 Enterprise Application Stores
78 Application Controls
80 Multinational Financial Services Firm Case Study

Chapter 8

Extreme Mobile Policy Enforcement

83 How the Right Policies and Data Analytics Can Ensure Proper Compliance
84 Get a Handle on Regulated Data
86 Enable Location-Based Controls
87 Enable a Centralized View
88 Data Analytics: Letting Your Data Tell Its Story
91 Monitoring for Compliance
92 Vepica Case Study

Enterprises Lag at Mobile Security, Growing Their Risk Profile Every Day

By John S. Chen
CEO and Executive Chairman, BlackBerry Ltd.

By now, organizations like yours have probably embraced mobile devices and apps for all of the business and productivity opportunities they bring. However, all of the hard-earned ROI and productivity gains you're dreaming about could disappear the moment a hacker successfully phishes your employees' account information via a crafty text message, or when your customers' financial data is stolen using passwords on an executive's lost device.

These nightmare scenarios are already rather common. According to a BlackBerry-commissioned survey of 800 CIOs and risk and compliance leaders last year, 59 percent admitted that the number of data breaches caused by mobile devices **had increased** in the past year (and keep in mind, those are only the ones they know about). As a result, 68 percent agreed that mobile devices are already the weakest link in their security framework.

Despite the admitted breaches, 61 percent of organizations continue to miscalculate or underestimate the risk caused by mobile, admitted their CIOs or risk and compliance managers. In other words: organizations, even those that are normally very conscientious about security, are doing very little when it comes to mobile security.

Clearly, there is plenty of catching up to do. What's your first move? I would suggest reading this guide book, *The Definitive Guide to Mobile Security*, cover to cover. Produced by BlackBerry security experts, the book provides a strategic overview of ALL the risks that your organization faces today in the mobile-first world.

Aimed at both business and IT decisionmakers, *The Definitive Guide to Mobile Security* also offers actionable tactics for planning and building a bullet-proof security architecture, and how to recover if breaches do occur. The guide is especially relevant to those who operate in high-security, regulated industries such as financial services, healthcare, government, etc.

After reading the Guide, I invite you to continue the conversation with one of the security experts here at BlackBerry, or visit BlackBerry.com to download other informative resources, and/or follow BlackBerry via bizblog.blackberry.com and BlackBerry4Biz to learn more tips on enterprise mobile security.

BlackBerry