

# Contents at a Glance

<b><i>Introduction</i></b> .....	<b>1</b>
<b><i>Part I: Living Securely in the Smart World</i></b> .....	<b>7</b>
Chapter 1: What's So Smart About a Phone, Anyway?.....	9
Chapter 2 : Why Do I Care? The Mobile Device Threat.....	33
Chapter 3 : Planning for Mobile Devices in the Enterprise .....	57
<b><i>Part II: Implementing Enterprise Mobile Security</i></b> .....	<b>77</b>
Chapter 4: Creating Mobile Device Security Policies .....	79
Chapter 5: Managing and Controlling Devices .....	105
Chapter 6: Conforming to Corporate Compliance Policies .....	127
<b><i>Part III: Securing Smart Device Access</i></b> .....	<b>147</b>
Chapter 7: Securing Data in Transit with VPNs .....	149
Chapter 8: Connecting to Wi-Fi Networks.....	177
<b><i>Part IV: Securing Each Smart Device</i></b> .....	<b>187</b>
Chapter 9: Device Security Component Overview .....	189
Chapter 10: Hacker Protection and Enforceable Encryption .....	209
Chapter 11: Protecting Against Loss and Theft .....	233
Chapter 12: Educating Users about Backing Up Data .....	247
Chapter 13: Securing Mobile Applications .....	263
<b><i>Part V: The Part of Tens</i></b> .....	<b>273</b>
Chapter 14: Top Ten Online Information Sources .....	275
Chapter 15: Top Ten Mobile Security Vendors.....	279
<b><i>Index</i></b> .....	<b>283</b>

<http://www.pbookshop.com>

# Table of Contents

.....

<b><i>Introduction</i></b> .....	<b>1</b>
About This Book .....	1
Foolish Assumptions .....	2
Conventions Used in This Book .....	2
How This Book Is Organized .....	3
Part I: Living Securely in the Smart World .....	3
Part II: Implementing Enterprise Mobile Security .....	4
Part III: Securing Smart Device Access .....	4
Part IV: Securing Each Smart Device .....	4
Part V: The Part of Tens .....	4
Icons Used in This Book .....	4
Where to Go from Here .....	5
<b><i>Part I: Living Securely in the Smart World</i></b> .....	<b>7</b>
<b>Chapter 1: What's So Smart About a Phone, Anyway?</b> .....	<b>9</b>
Exploring Different Mobile Devices .....	10
Smartphones and tablets .....	10
Laptops and netbooks .....	13
Other computing devices .....	14
Examining Operating Systems for Mobile Devices .....	14
Apple iOS .....	15
Google Android .....	17
RIM BlackBerry OS .....	18
RIM BlackBerry Tablet OS .....	18
Microsoft Windows Mobile and Windows Phone .....	19
Nokia Symbian .....	19
HP Palm webOS .....	20
MeeGo .....	20
Samsung bada .....	21
Discovering Data Connections .....	21
Applications Galore: Exploring Mobile Device Applications .....	22
E-mail and messaging .....	23
Web-based applications .....	23
Client/server applications .....	23
Standalone applications .....	24



Allowing Smartphones onto Your Network .....	24
Educating yourself on the risks .....	25
Scoping your deployment.....	25
Creating a mobile device security policy .....	25
Determining device configuration policies .....	25
Figuring out how you'll connect devices to your network(s).....	26
Devising an endpoint security strategy .....	26
Planning a strategy to deal with loss and theft.....	26
Seeking vendor info and requests for proposals .....	27
Implementing a pilot.....	27
Assessing and reevaluating at regular intervals .....	27
Introduction: AcmeGizmo Enterprise Smartphone	
Deployment Case Study .....	28
Exploring legacy smartphone deployment.....	28
Enter the smartphone explosion .....	30
<b>Chapter 2: Why Do I Care? The Mobile Device Threat .....</b>	<b>33</b>
Recognizing the Scope of the Threat .....	34
Loss, theft, and replacement.....	34
Really off-site data storage .....	35
Free (but not necessarily nice) apps.....	36
Network access outside of your control.....	36
Understanding the Risks.....	37
Opening the door to hackers.....	38
Compromising your business communications .....	41
Endangering corporate data.....	42
Infesting enterprise systems by using location-based services ....	46
Assessing the Arsenal .....	48
To manage or not to manage.....	49
Where the need for compliance comes in .....	49
Mobile security apps start to emerge .....	50
Planning to Sustainably Keep the Threat at Bay .....	50
Establish enforceable policies .....	50
Evaluate tools without biases .....	51
Secure the location.....	52
Mobile security 101 classes.....	53
Turning mobile devices into allies.....	54
<b>Chapter 3: Planning for Mobile Devices in the Enterprise .....</b>	<b>57</b>
Managing the New Wave of Mobile Devices.....	58
Support the cutting-edge devices .....	59
More than just e-mail.....	60
Who moved my application?.....	62
Updating your mobility policies .....	63

Adapting to the New Challenges of Mobile Devices.....	64
Protecting mobile devices from malware.....	65
Managing device policies remotely.....	68
Enforcing granular access control.....	70

## ***Part II: Implementing Enterprise Mobile Security..... 77***

### **Chapter 4: Creating Mobile Device Security Policies..... 79**

Recognizing the Importance of Enforceable Security Policies .....	79
Understanding Device Policies .....	81
Policies for physical device protection .....	83
Policies for device backup and restore.....	85
Using Provisioning Policies to Manage Devices .....	89
Upgrade, downgrade, and software installation policies .....	89
Profile settings policies.....	91
Decommissioning policies.....	94
Creating Effective Monitoring Policies.....	95
Protecting Devices with Application Policies .....	97
Case Study: AcmeGizmo Mobile Device Security Policy .....	101

### **Chapter 5: Managing and Controlling Devices..... 105**

Managing Your Mobile Devices .....	106
Managing devices over the air.....	106
Configuring security policies.....	111
Open Mobile Alliance Device Management .....	118
Exchange ActiveSync.....	119
Controlling Applications.....	120
Pros and cons of consumer app stores .....	120
Provisioning applications to mobile devices .....	121
Blacklisting and removing applications .....	122
Case Study: AcmeGizmo Application Control Deployment .....	123
Your password, please.....	123
Network settings .....	125
Other settings.....	125
Application provisioning .....	126

### **Chapter 6: Conforming to Corporate Compliance Policies..... 127**

Which Devices Are Personal, and Which Are Corporate-Owned .....	128
Setting Passcodes on Mobile Devices.....	129
Encrypting the Contents of the Device.....	131
Requiring VPN on the Device.....	132
Protecting the Device from Viruses .....	134

Protecting the Device from Loss and Theft .....	136
Managing Devices at Scale .....	137
Backing Up the Contents of the Device .....	139
Monitoring and Controlling Contents of the Device .....	141
Case Study: AcmeGizmo Compliance Requirements.....	143
Operating system compliance.....	143
Password compliance .....	143
Encryption compliance.....	144
VPN and endpoint security compliance .....	144
Loss and theft protection .....	144

## ***Part III: Securing Smart Device Access .....*** 147

### **Chapter 7: Securing Data in Transit with VPNs .....** 149

Comparing IPSec VPNs and SSL VPNs .....	150
Validating User Identity for VPN Access .....	151
Authenticating VPN users.....	152
Determining a user's role.....	154
Discriminating by Device Profile .....	155
Profiling devices and applying policies .....	157
Providing access based on device profile .....	160
Implementing custom policies .....	160
Providing Application Access .....	161
Enabling access to e-mail.....	162
Providing web application access .....	162
Accessing full client/server applications.....	163
Providing Users an Appropriate Level of Access .....	163
Securely accessing e-mail, calendar, and contacts .....	164
Accessing web-based applications.....	166
Allowing users to leverage client/server applications.....	167
Case Study: AcmeGizmo SSL VPN Rollout for Smartphones.....	171
Employee authentication .....	172
Accessing the network with SSL VPN.....	173

### **Chapter 8: Connecting to Wi-Fi Networks .....** 177

What's Wi-Fi, and Why Bother? .....	177
Which Wi-Fi Networks Should Users Connect To?.....	178
Open or insecure networks .....	178
Encrypted Wi-Fi networks.....	179
VPN on a Wi-Fi network.....	180
Wi-Fi Connections from Mobile Devices .....	180
Apple iPhones, iPads, and iPods.....	180
Connecting to Wi-Fi with Android devices .....	182
BlackBerry devices .....	183
Implementing Wi-Fi Policies .....	184

## ***Part IV: Securing Each Smart Device* ..... 187**

### **Chapter 9: Device Security Component Overview ..... 189**

Knowing Smartphone Security Components .....	189
Understanding On-Device Anti-X Protection.....	191
Antispyware.....	191
Antivirus.....	193
Antiphishing .....	194
Antispam.....	196
Using Backup and Restore Capabilities .....	197
Adding Loss and Theft Protection.....	199
Encryption and authentication techniques.....	200
Immobilizing techniques.....	200
Recovery techniques.....	200
Controlling and Monitoring Applications.....	201
Methods to control and monitor applications.....	202
Identifying harmful applications.....	202
Enterprise Management of Mobile Devices.....	203
Device deployment.....	203
Device discovery.....	204
Device provisioning.....	205
Device monitoring.....	205
Compliance enforcement.....	206

### **Chapter 10: Hacker Protection and Enforceable Encryption ..... 209**

Getting to Know the On-Device Security Components .....	209
Keeping Devices Safe with On-device Firewalls.....	211
Small footprint.....	212
Efficient battery usage.....	213
Dynamic adaptation to changing usage.....	214
Protecting Against Viruses .....	215
Firewalls and virus-based attacks.....	218
Virtual device antivirus solutions.....	219
Reducing Spam .....	220
Service provider assistance .....	221
Choosing an antispam solution.....	221
Global operator initiative to combat spam .....	222
Preventing Intrusion.....	223
Using Enforceable Encryption .....	227
Encrypting all outbound and inbound communication.....	227
Encrypting only enterprise traffic.....	227
Using carrier-provided voice encryption.....	229
Case Study: AcmeGizmo Endpoint Security Deployment.....	230
Endpoint security .....	231
Device encryption.....	232
Flash forward.....	232

**Chapter 11: Protecting Against Loss and Theft . . . . . 233**

Taking Precautions before Loss or Theft .....	233
Educating Users about Securing Data on a Lost Phone.....	235
Protecting personal Apple iOS devices.....	235
Protecting personal Symbian devices.....	237
Protecting personal Android devices.....	239
Protecting personal Windows Mobile and Windows Phone 7 Devices .....	240
Protecting personal Blackberry devices.....	241
Exploring Enterprise-Grade Solutions for Various Platforms .....	241
Enterprise-grade solutions for Apple iOS .....	241
Enterprise-grade solutions for Symbian .....	242
Enterprise-grade solutions for Android.....	242
Enterprise-grade solutions for Windows Mobile and Windows Phone 7 .....	242
Enterprise-grade solutions for Blackberry devices.....	243
Deploying Enterprise-Wide Loss and Theft Protection .....	243
Case Study: AcmeGizmo's Lost or Stolen Device Recovery.....	244

**Chapter 12: Educating Users about Backing Up Data . . . . . 247**

Backing Up Data from Smartphones .....	247
Instructing Users on Backing Up Their Devices .....	249
Backing up iPhones and iPads .....	249
Backing up Android devices.....	250
Backing up BlackBerry devices.....	251
Backing up Nokia devices .....	252
Backing up Windows Phone 7 devices.....	253
Instructing Users on Restoring Data to Their Devices .....	254
Restoring data from iPhones and iPads.....	254
Restoring data from Android devices .....	255
Restoring data from BlackBerry devices .....	256
Restoring data from Nokia devices.....	256
Restoring data from Windows Phone 7 devices .....	256
Instructing Users on Transferring Data to New Devices .....	257
Transferring data between iPhones and iPads .....	257
Transferring data between Android devices.....	258
Transferring data between BlackBerry devices.....	258
Transferring data between Nokia Symbian devices .....	259
Exploring Corporate Solutions for Backup and Restore .....	259
Case Study: AcmeGizmo Backup and Restore Use Cases .....	261

**Chapter 13: Securing Mobile Applications . . . . . 263**

- Understanding the Importance of a Sandbox ..... 263
- App Security on Various Platforms ..... 264
  - App security on BlackBerry devices ..... 265
  - App sandboxing on Apple iOS devices ..... 266
  - Android operating system security ..... 267
- Exploring Virtualization for Mobile Devices ..... 268
- Accounting for Personal Devices at Work ..... 269
- Sandboxing Combined with On-Device Security ..... 270

***Part V: The Part of Tens* ..... 273**

**Chapter 14: Top Ten Online Information Sources... 275**

- Tech SANS ..... 275
- Dark Reading ..... 276
- F-Secure Security Threat Summaries ..... 276
- Infosecurity Network ..... 276
- National Institute of Standards and Technology (Security Research)... 276
- Vendors' Websites ..... 277
- ICSA labs ..... 277
- CERT ..... 278
- US-CERT ..... 278
- GSM Association ..... 278

**Chapter 15: Top Ten Mobile Security Vendors . . . . . 279**

- AirWatch ..... 279
- Good Technology ..... 280
- Juniper Networks ..... 280
- Mobile Active Defense ..... 280
- McAfee ..... 281
- MobileIron ..... 281
- Sybase ..... 281
- Symantec ..... 281
- Tangoe ..... 282
- Zenprise ..... 282

***Index* ..... 283**

<http://www.pbookshop.com>