

Mobile Device Security

A Comprehensive Guide to Securing
Your Information in a Moving World

STEPHEN FRIED

UNIVERSITÄT
LIECHTENSTEIN

Bibliothek



CRC Press

Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
AN AUERBACH BOOK

Contents

Acknowledgments.....	xiii
About the Author.....	xv
Trademarks.....	xvii
Introduction.....	xix
How Did We Get Here?.....	xxi
The Beginning of the End.....	xxii
Where We Are Now.....	xxiii
The Real Problems.....	xxiv
• What You'll Learn in This Book.....	xxv
A Note on Technology and Terminology.....	xxvi
Final Thoughts.....	xxvii
1 What Are You Trying to Protect?.....	1
Finding a Definition for Mobile Data...':.....	2
Mobile Data Scenarios.....	4
Other Factors to Consider.....	5
Defining a Mobile Device.....	7
Distinct, but Intertwined.....•.....	10
Movable Data, Movable Risk.....	11
Following the Path.....	13
The Inverse Distance Principle...".....	15
The Effect on Our Approach.....	16
Conclusion.....	18
Action Plan.....	19
Notes.....	20
2 It's All about the Risk.....	21
Loss or Disclosure of Data to Inappropriate Persons.....	24
Loss of Money.....	26
Loss of Trust or Damage to Your Reputation.....	28
You Are Not Immune.....	29

Risk, Threat, and Value.....	30
Risk: Lost or Stolen Mobile Devices.....	31
Risk: Inability to Secure Devices to Desired Level, Granularity, or Uniformity.....	33
Risk: Access to Internal Information from Uncontrolled Devices....	35
Risk: Introduction of Malware into the Environment from Unprotected Mobile Devices.....	36
Risk: Information Loss Due to Uneducated, Inattentive, or Uncaring Users.....	38
Risk: Lack of Compliance with the Legislation du Jour.....	41
Evaluating Your Risks.....	44
How Valuable Is Your Data?.....	47
What about Countermeasures?.....	49
Conclusion.....	49
Action Plan.....	50
Notes.....	51
3 The Many Faces of Mobility.....	53
Following the Bits.....	54
Portable Storage Devices.....	58
Portable Storage Devices: Intentional Mobility.....	59
Portable Storage Devices: Unintentional Mobility.....	60
Tape Storage.....	62
Tapes: Intentional Mobility.....	62
Tapes: Unintentional Mobility.....	62
Dual-Use Devices.....	63
Dual-Use Devices: Intentional Mobility.....	64
Dual-Use Devices: Unintentional Mobility.....	64
Smartphones and Personal Digital Assistants.....	65
Smartphones and PDAs: Intentional and Unintentional Mobility ...	65
Optical Media (CD and DVD).....	67
Optical Media: Intentional Mobility.....	67
Optical Media: Unintentional Mobility.....	67
Portable Computers.....	68
Portable Computers: Intentional Mobility.....	68
Portable Computers: Unintentional Mobility.....	68
Electronic Mail.....	69
E-mail: Intentional Mobility.....	70
E-mail: Unintentional Mobility.....	72
Instant Messaging and Text Messaging.....	73
IM and Texting: Intentional Mobility.....	74
IM and Texting: Unintentional Mobility.....	74
Conclusion.....	75

Action Plan.....	76
Notes.....	77
4 Data at Rest, Data in Motion.....	79
It's All a Matter of Physics.....	79
More Definitions.....	80
Protecting Data at Rest.....	82
Physical Protection Methods.....	82
Keep the Storage Device Hidden.....	83
Split the Data onto Multiple Devices.....	84
Use a Locked Container.....	85
Use Tamper-Proof or Tamper-Evident Containers.....	85
Use a Special Courier.....	87
Use Obscurity to Your Advantage.....	87
Physical Protection Summary.....	89
Logical Protection Mechanisms.....	89
Authentication.....	89
Access Controls.....	92
Encryption.....	93
Effective Data Management.....	94
• The Problem of Heterogeneous Information.....	95
Protecting Data in Motion.....	96
Physical Controls.....	97
Logical Protections.....	98
The Rise of Monocultures.....	98
Insecurity in the Links.....	99
Multiple Networks Mean Multiple Data Paths.....	101
Establishing PC Restrictions.....	103
Conclusion.....	103
Action Plan.....	105
Notes.....	106
5 Mobile Data Security Models.....	107
A Device-Centric Model.....	108
Access Control.....	108
Data-Flow Restrictions.....	109
Device Management.....	110
Selective Feature Restrictions.....	112
Logging and Auditing Capabilities.....	114
Defining Your Scope.....	115
Defining Acceptable Use Cases.....	117
Who Gets Access?.....	117
Keeping Up with Device Technology.....	118
Device-Centric Challenges.....	119

Contents

A Data-Centric Model.....	120
Data-Centric Access Controls.....	121
Blocking Certain Data Types.....	122
Encryption.....	124
Information Rights Management.....	128
Data-Centric Challenges.....	131
Which Model Do You Choose?.....	132
Conclusion.....	136
Action Plan.....	136
6 Encryption.....	139
Uses for Encryption.....	140
The Importance of Standards.....	140
Symmetric Encryption.....	141
Asymmetric Encryption.....	143
When to Use Encryption.....	146
Infrastructure and Workflow Compatibility.....	147
Encryption Impediments.....	149
Mobile Data Encryption Methods.....	150
Full-Disk Encryption.....	151
File- and Directory-Based Encryption.....	152
Virtual Disk and Volume Encryption.....	154
Hardware-Encrypted Storage Drives.....	155
Tape Encryption.....	156
Key Management.....	158
Data Protection vs. Data Recovery.....	160
Conclusion.....	162
Action Plan.....	163
Notes.....	164
7 Defense-in-Depth: Mobile Security Controls.....	165
Countermeasures as Controls.....	166
Directive and Administrative Controls.....	168
Policies.....	168
Administrative Changes.....	169
Deterrent Controls.....	170
Policies.....	170
Education and Awareness.....	171
Organizational Culture.....	174
Preventive Controls.....	175
Encryption.....	176
Trusted Platform Modules.....	176
Content Filtering and Data Loss Prevention.....	177

Desktop Virtualization.....	179
Centralized Device Management.....	181
Detective Controls.....	181
The Importance of Logs.....	182
Auditing as a Detective Control.....	184
Physical Security.....	184
Conclusion.....	185
Action Plan.....	189
Notes.....	189
8 Defense-in-Depth: Specific Technology Controls.....	191
Portable Computer Controls.....	192
Antimalware Services.....	192
Workstation-Based Firewalls.....	193
Standard Configurations.....	193
VPN and Multifactor Authentication.....	194
Network Access Control.....	195
Disabling Automatic Program Execution.....	196
Removing Unnecessary Data.....	196
Physical Protection.....	197
• Portable Storage Devices.....	198
Dual-Use Devices.....	199
Smartphones and PDAs.....	199
Optical Media.....	200
E-mail.....	201
Instant Messaging (IM) and Text Messaging.....	205
Conclusion.....	206
Action Plan.....	211
Note.....	211
9 Creating a Mobile Security Policy.....	213
Setting the Goal Statement.....	215
Mobile Device Policy Issues.....	217
Device Ownership.....	219
Device Management.....	222
Device Personalization.....	222
Mobile Data Issues.....	223
Option 1: Data Can Be Moved to Any Mobile Device.....	223
Option 2: Data Is Not Allowed to Be Moved to Any Mobile Device.....	224
Option 3: Data Is Allowed to Be Moved to Only Approved Devices.....	225
Option 4: Only Certain Types of Data Can Be Transferred to Mobile Devices.....	226

Option 5. All Data Transferred to a Mobile Device Must Have Minimum Security Protections.....	227
Defining Technology Standards.....	228
End-User Standards.....	229
Device Standards.....	230
Data Protection Standards.....	232
When Are Protections Required?.....	233
Conclusion.....	233
Action Plan.....	234
10 Building the Business Case for Mobile Security.....	237
Identifying the Catalyst.....	239
Forward-Thinking Leadership.....	239
Recent Incidents or Losses.....	240
Fear of Publicity and Reputational Damage.....	241
Audit Findings.....	242
Legislative or Regulatory Changes.....	243
Contractual or Business Obligations.....	243
Alignment with Company Objectives.....	244
Determining the Impact of the Problem.....	245
• Financial Losses.....	246
Reputational Damage.....	247
Cost of Remediation and Cleanup.....	248
Operational Impact.....	248
Describe the Current State of Controls.....	250
The Proposed Solution.....	252
Program Time Line.....	255
Financial Analysis.....	257
Calculating the Return on Investment.....	258
Alternatives Considered.....	260
Conclusion.....	261
Action Plan.....	263
Index.....	J.....265