Contents

Acknowledgments **iv**

Chapter 1: Security—The Reasons You're Reading This Book **1**
Evaluating Your Risks 3
Confidentiality 4
Integrity 4
Availability 5
Privacy 5
Evaluating the Threats 7
Managing the Strategic Issues 7
Control Access to Applications, Data, and Systems 8
Review Requirements and Maintain Compliance 9
Getting Started 9
Don't Close the Book 11
Don't Get Overwhelmed 11

Chapter 2: Policies and Procedures **13**
Your Security Policy 14
Physical Security 14
Responsible Parties 15
Data Classification 15
Network Connections 19
Application Design 20
BYOD 20

Social Media 21
Platform-Specific Issues 21
Employee Guidelines 21
Notification, Enforcement, and Compliance 22
Business Events and Procedures 23
Getting Started with Your Policy 24
Legal Review 25

Chapter 3: Security at the System Level **27**
The System Security Level 27
System Value QSECURITY 28
Security Level 20 28
Security Level 30 29
Security Level 40 31
Security Level 50 34
Moving to Security Level 40 or 50 36
Security-Related System Values 38
General Security System Values 38
Password-Related System Values 60
Audit-Related System Values 75
Locking Down Security-Related System Values 84
A Helpful Tool 84

Chapter 4: The Facts About User Profiles **85**
What Are User Profiles? 86
User Profile Attributes 87
USRPRF (User Profile) 89
PASSWORD (User Password) 91
PWDEXP (Set Password to Expired) 93
LCLPWDMGT (Local Password Management) 93
PWDEXPITV (Password Expiration Interval) 94
PWDCHGBLK (Block Password Change) 95
STATUS (Profile Status) 96
USRCLS (User Class) and SPCAUT (Special Authority) 97
Initial Sign-on Options 101
System Value Overrides 104
Group Profiles 104

UID and GID 108
USREXPDATE (User Expiration Date) and USREXPITV (User Expiration Interval) 108
AUT (Authority) 108
Private Authorities and User Profiles 109
Helpful Tools 109
Navigator for i 111
Copying User Profiles 112
Validation List Users 113
Security Implications of Validation List Users 124

Chapter 5: Service Tools Security 127
Service Tools User IDs 128
Service Tools User ID Passwords 129
Service Tools Functional Privileges 132
Service Tools Features 138
Device Profiles 139
The Work with System Security Panel 141
Monitoring Service Tools Use 142
Service Tools Security Recommendations 144

Chapter 6: Object-Level Security 147
Private Authorities 148
Object Authorities 149
Data Authorities 150
Authority Relationships 151
Authority Groupings 152
Group Profiles 153
Multiple Group Profiles 153
Why Grant Authority to Group Profiles? 154
Public Authority 155
Establishing Public Authority 155
Using Default Public Authority 158
Authorization Lists 160
How IBM i Checks Authority 162
Authority Checking Example: Precedence Between Users and Groups 165
Authority Cache 166

Adopted Authority 166
Adopted Authority Example 168
Authorities and Save/Restore Functions 170
Object Ownership 172
Limit User Function (Application Administration) 174
Row and Column Access Control (RCAC) 179
Prerequisites 179
Understanding RCAC 181
Column Masks 185
Column Mask Considerations 186
Managing RCAC 186
Save/Restore Considerations 187
More Information 188
Summary 188
Authority Collection 189
Helpful Tools 193
Navigator for i 193

Chapter 7: Security Considerations for the IFS 195
IFS Authorities 196
Managing Authorities to IFS Objects 198
File Attributes 200
Adopted Authority and the IFS 201
Auditing Objects in the IFS 202
File Shares: Accessing Objects in the IFS 202
Gotchas and Helpful Hints 205
General Cautions 205
Creating New Objects 205
Copying Objects 206
CPYTOSTMF and CPYTOIMPF 207
Virus Scanning 207
Security Recommendations 208
**PUBLIC Authority for Application and User Directories* 208
**PUBLIC Authority for IBM-Supplied Directories* 208
Determining Appropriate Authority 209
Home Directory 210

Web Applications 210
QPWFSERVER Authorization List 211
Review (and Remove) File Shares 211
IBM i NetServer 212
Final Advice 213
Helpful Tools 213

Chapter 8: Securing Your Printed Output **215**
Security-Related Output Queue Attributes 216
DSPDTA (Display Data) 216
OPRCTL (Operator Control) 217
AUTCHK (Authority Check) 217
AUT (Authority) 218
**SPLCTL Special Authority* 218
Output Queue Ownership 219
Sample Output Queue Security Implementation 220
Helpful Tools 222
Navigator for i 222

Chapter 9: Encryption **223**
Encryption Basics 223
Public Key Infrastructure 224
Transmission of Data 226
Encrypting Data in Files 226
Identify the Scope of Your Project 227
Architecting Your Application to Use Encryption 229
The Key Is Key Management 230
Encrypting Backup Media 232
What IBM Provides 233
Encrypted Auxiliary Storage Pools 233
Disaster Recovery Considerations 233
Success Depends on Planning 234
Helpful Resources 234

Chapter 10: Connecting to the System **235**
Physical Security 235
System Values 236

*IOSYSCFG Special Authority 236
Network Security Attributes 237
JOBACN 237
PCSACC 238
DDMACC 238
Security Considerations for TCP/IP 238
Starting TCP/IP Servers 239
Securing Ports 240
Internal Addresses 241
IP Packet Filtering 241
NAT 242
FTP 242
SMTP 244
POP 245
DNS 246
REXEC 246
SNMP 247
SNTP 247
DRDA and DDM 247
Security Considerations for PCs and Mobile Devices 250
Access Client Solutions 250
ODBC Security Considerations 253
IBM i Access for Web 253
Using Exit Points 255
Management Central 256
Secure Communications 256
Digital Certificates 257
Transport Layer Security 257
Digital Certificate Manager 261
Virtual Private Networks 261
Secure Shell 262
Wireless Considerations 262
Helpful Tools 263
Navigator for i 263
IBM Navigator for i 264

Chapter 11: Internet Security **265**
Determine Your Risk 265
The Process 266
Corporate Security Policy 267
Internet Service Provider 268
Firewalls 268
System Values 270
User Profiles 272
Resource Security 272
Controlling What Goes On 273
Secure Web Applications 274
Exit Programs 276
Monitoring 277
Intrusion Detection 277
Security Configuration 278
Testing and Evaluation 281
Business Contingency Plan 282
Be Careful Out There 282

Chapter 12: Evaluating Applications' Current Implementations and Designing New Ones 283
From the Beginning 284
Design Considerations 285
What Roles Will Use the Application? 286
Common Authorization Schemes 287
Application Ownership 293
Which Profile Runs the Application, and Is There Adequate Logging? 294
Does the Application Require a "Powerful" Profile? 294
What Kind of Audit Trail Does the Application Require? 295
Implementation Details 296
Set IBM i Authorities 296
*Define *PUBLIC Authority* 296
Security Questionnaire for Vendors 297
Secure Job Descriptions 299
Manage Your Library List 299
Make Library-Qualified Calls 299
Don't Store Passwords in Clear Text 300

Testing, Testing 300
Moving Forward 301

Chapter 13: Role-Based Access 303
Roles 303
Defining the Roles 304
Group Profiles 305
Why Group Profiles? 307
Implementation 307

Chapter 14: Role-Based Access for IT 309
Security and Your IT Staff 309
Identify the Roles 310
Define a Secure Environment for Each Business Function 311
Operator 311
Network Administrator for IBM i 314
Help Desk 314
Programmer/Analyst 315
System and Security Administrators 318
Security for Vendors and Consultants 319
Vendor Support 320
Consultant Practices 320
Role-Based IT Access 321

Chapter 15: Auditing 323
The History Log 325
History Log Housekeeping 326
Inside Information 326
The Security Audit Journal 327
The Audit Journal 328
Auditing Controls 329
System-Wide Auditing 329
Other Auditing Values 333
User Auditing 334
Object Auditing 335
Object Auditing for New Objects 338
Event-Auditing Recommendations 338

Auditing Controls Security Recommendations 339
System and User Event-Auditing Security Recommendations 339
Object-Auditing Recommendations 339
Working with the Audit Journal 340
Understanding Journal Entry Formats 340
Displaying and Printing Audit Journal Entries 343
Using the DSPAUDJRNE Command to Display Entries 343
Using the DSPJRN Command to Display Entries 345
Using the CPYAUDJRNE Command 347
Reporting on Activities from the Information in the Audit Journal 348
Benefits of the IBM i Architecture 350
Helpful Tools 350
Navigator for i 351

Chapter 16: Implementing Object-Level Security 353
Determine the Scope of Your Project 354
High-Level Design of the Architecture 355
Building the Big Picture 356
Collecting the Information 358
Dynamic SQL 361
Decision Points 362
Owning All Application Objects Rather Than Being Authorized 362
What Adopts 362
Authorization Lists 364
**PUBLIC Authority* 365
Queries 367
Making Changes to the Application 368
Rolling Out the Changes 370
Changes to Change Management 371
When Something Breaks: Debugging and Recovery Techniques 371
Making Sure the Changes "Stick" 373
Gotchas 373
Summary 374

Chapter 17: Security Administration 375
Remove Obsolete Objects 375

System Values 376
User Profiles 376
Managing Authorities 379
Regular Reviews 379
Controlling Who Can Do What 380
Integrated File System (IFS) 380
Stay Current 381
Summary 381

Chapter 18: Maintaining Compliance 383
Evaluating the Key Areas 384
System Values 385
User Profiles 385
Object Authority 387
An Annual Security Assessment 388
Regular Reviews 389
Group Profile Membership and Special Authority Assignments 390
Authorization Lists 390
Policies and Processes 391
Summary 392

Chapter 19: Preparing for the Worst: Creating a Security Incident Response Plan 393
Be Prepared 393
Assembling the Incident Response Team 394
Responding to an Incident 395
Data Preservation 396
Performing the Investigation 396
Be Proactive 397
Make Sure You're Saving the Right Information 397
Saving Security Data 397
Restoring Security Data 398
Recreating the System After a Breach 400

Chapter 20: Creating a Security Awareness Program 401
What Method Do I Use to Communicate? 402
Getting Started 403

Index 407