

Contents

Acknowledgments	v
Chapter 1: Security—The Reasons You’re Reading This Book	1
Evaluating Your Risks.....	2
Confidentiality	2
Integrity.....	3
Availability	3
Privacy	4
Evaluating the Threats.....	4
Get Management Buy-in	5
Control Access to Applications, Data, and Systems	6
Review Requirements and Maintain Compliance.....	7
Getting Started.....	7
Chapter 2: Policies and Procedures	9
Your Security Policy	10
Physical Security.....	10
Data Classification.....	11
What Classifications Should You Use?.....	12
Who’s Responsible for Classifying Data?.....	13
Data Ownership	13
Why Not IT?.....	14
Network Connections.....	14
Application Design	15
BYOD	16
Social Media	16
Platform-Specific Issues	16
Employee-Specific Policies	17
Notification, Enforcement, and Compliance.....	18
Getting Started with Your Policy	19
Legal Review.....	19

Chapter 3: Security at the System Level	21
The System Security Level.....	21
System Value QSECURITY	21
Security Level 20	22
Security Level 30	23
Security Level 40	24
State and Domain Restrictions	24
Use of Restricted MI Instructions.....	25
Privilege Escalation.....	25
Why Use Security Level 40?	26
Security Level 50	26
Message Restrictions and Pointer Removal	26
Prevention of Control-Block Modification.....	27
Why Use Security Level 50?.....	27
Moving to Security Level 40 or 50 from Level 30	28
Moving to Security Level 40 or 50 from Level 20	29
Security-Related System Values	30
General Security System Values.....	30
Password-Related System Values.....	52
Audit-Related System Values.....	61
Locking Down Security-Related System Values	69
A Helpful Tool	69
Chapter 4: The Facts About User Profiles	71
What Are User Profiles?.....	71
User Profile Attributes.....	72
USRPRF (User Profile).....	72
PASSWORD (User Password).....	77
PWDEXP (Set Password to Expired)	78
PWDEXPITV (Password Expiration Interval).....	79
PWDCHGBLK (Block Password Change)	80
STATUS (Profile Status)	80
USRCLS (User Class) and SPCAUT (Special Authority).....	81
Initial Sign-on Options.....	86
LMTCPB (Limit Capabilities).....	87
System Value Overrides.....	89
Group Profiles.....	89
Creating Group Profiles.....	89
Assigning a Group to a User Profile.....	91
UID and GID.....	93
USREXPDATE (User Expiration Date) and USREXPITV (User Expiration Interval) ...	93

AUT (Authority).....	93
Private Authorities and User Profiles	94
Helpful Tools.....	94
Navigator for i	96
Copying User Profiles	98
SQL Views in QSYS2	98
Validation List Users.....	99
Security Implications of Validation List Users.....	107
Chapter 5: Service Tools Security.....	109
Service Tools User IDs.....	109
Service Tools User ID Passwords.....	111
Default Password Policy Details	112
Alternate Password Policy Details—PWLVL 2.....	113
Additional Password Composition Rules.....	114
Choosing a Password Policy	114
Service Tools Functional Privileges.....	114
Linking Service Tools IDs	118
Managing Service Tools IDs Using IBM i Commands	120
Device Profiles	122
The Work with System Security Panel.....	123
Monitoring Service Tools Use.....	125
Service Tools Security Recommendations	126
Chapter 6: Object-Level Security	129
Private Authorities.....	129
Object Authorities.....	130
Data Authorities	132
Authority Relationships	133
Authority Groupings	133
Group Profiles	135
Multiple Group Profiles	135
Public Authority	136
Establishing Public Authority	136
Using Default Public Authority	139
Authorization Lists	141
How IBM i Checks Authority	143
Authority Checking Example: Precedence Between Users and Groups.....	146
Authority Cache	147
Adopted Authority.....	147
Adopted Authority Example	149

Authorities and Save/Restore Functions.....	151
Object Ownership.....	152
Application Administration (Function Usage)	154
Row and Column Access Control (RCAC).....	157
Prerequisites.....	158
Understanding RCAC.....	160
Programmer Considerations	162
Column Masks	162
Column Mask Considerations	163
Managing RCAC	164
Save/Restore Considerations.....	165
More Information.....	165
Summary	166
Helpful Tools.....	166
Navigator for i	166
SQL Views in QSYS2	167
Chapter 7: Security Considerations for the IFS	169
IFS Authorities	171
Managing Authorities to IFS Objects.....	172
File Attributes	174
Adopted Authority and the IFS.....	175
Auditing Objects in the IFS	176
Gotchas and Helpful Hints	177
General Cautions.....	177
Creating New Objects	177
Copying Objects.....	178
CPYTOSTMF and CPYTOIMPF.....	178
General Security Recommendations	179
*PUBLIC Authority for Application and User Directories	179
*PUBLIC Authority for IBM-Supplied Directories	179
Determining Appropriate Authority.....	180
Home Directory	181
Web Applications.....	181
QPWFSERVER Authorization List.....	181
File Shares: Accessing Objects in the IFS.....	182
The Risk of File Shares.....	183
Review (and Remove) File Shares.....	184
IBM i NetServer.....	184
To Virus Scan or Not Virus Scan?.....	185
Tips for Avoiding Malware	186

Final Advice.....	187
Helpful Tools.....	187
SQL Views	187
Chapter 8: Securing Your Printed Output	189
Security-Related Output Queue Attributes.....	190
DSPDATA (Display Data)	190
OPRCTL (Operator Control).....	191
AUTCHK (Authority Check).....	191
AUT (Authority).....	191
*SPLCTL Special Authority	192
Output Queue Ownership	193
Sample Output Queue Security Implementation	194
Helpful Tools.....	195
Navigator for i	196
SQL Views	196
Chapter 9: Encryption	197
Encryption Basics.....	197
Public Key Infrastructure	198
Transmission of Data.....	199
Encrypting Data in Files.....	200
Identify the Scope of Your Project	201
The Key Is Key Management	202
Key Generation.....	202
Separation of Duties	203
Storing the Keys.....	203
Controlling Access to Encryption/Decryption Routines	203
Backing Up the Keys.....	203
Changing the Keys	204
Encrypting Backup Media.....	204
What IBM Provides	205
Disaster Recovery Considerations.....	205
Success Depends on Planning	205
Chapter 10: Connecting to the System	207
Physical Security	207
System Values	208
*IOSYSCFG Special Authority.....	208
Secure Communications.....	208
Digital Certificates	209

Transport Layer Security	209
System Values for Secure (Encrypted) Communications	210
Digital Certificate Manager	212
Security Considerations for TCP/IP	213
Starting TCP/IP Servers	213
Session Time-Out Value.....	214
Securing Ports	214
Internal Addresses.....	215
IP Packet Filtering.....	215
NAT	216
FTP.....	216
Secure Shell	218
SMTP	219
POP	219
DNS	220
REXEC	221
SNMP.....	221
SNTP.....	222
DRDA and DDM	222
DDM	222
Securing DDM	224
Reducing the Risk When a Password Is Not Required	226
Security Considerations for PCs and Mobile Devices.....	226
Access Client Solutions	227
Data Transfer and Remote Command Issues	227
Host Servers	228
Limiting What Users See from the Desktop.....	228
ODBC Security Considerations	229
IBM i Access for Web	229
Using Exit Points.....	230
Virtual Private Networks	231
Wireless Considerations	231
Network Security Attributes.....	233
JOBACN	233
PCSACC.....	234
DDMACC.....	234
Helpful Tools.....	235
Navigator for i	235
Chapter 11: Internet Security	237
Determine Your Risk.....	237

The Process.....	238
Corporate Security Policy.....	238
Internet Service Provider.....	240
Firewalls.....	240
System Values.....	242
User Profiles.....	244
Resource Security.....	244
Controlling What Goes On.....	245
Secure Web Applications.....	246
Exit Programs.....	248
Monitoring.....	248
Intrusion Detection.....	248
Security Configuration.....	250
Testing and Evaluation.....	250
<i>Security Considerations for Outsourcing and the Cloud</i>	251
Business Contingency Plan.....	253
Be Careful Out There.....	253
Chapter 12: Evaluating Applications' Current Implementations and Designing New Ones.....	255
From the Beginning.....	256
Design Considerations.....	257
What Roles Will Use the Application?.....	258
Common Authorization Schemes.....	258
Menu Access Control.....	259
Excuses and Justifications.....	261
Authorization Schemes That Are Secure.....	262
Application Ownership.....	264
Which Profile Runs the Application, and Is There Adequate Logging?.....	265
Does the Application Require a "Powerful" Profile?.....	265
What Kind of Audit Trail Does the Application Require?.....	266
Implementation Details.....	267
Set IBM i Authorities.....	267
<i>Security Questionnaire for Vendors</i>	268
Define *PUBLIC Authority.....	268
Secure Job Descriptions.....	270
Manage Your Library List.....	270
Make Library-Qualified Calls.....	270
Don't Store Passwords in Clear Text.....	271
Testing, Testing.....	271
Moving Forward.....	272

Chapter 13: Role-Based Access	273
Roles	273
Defining the Roles	274
Group Profiles	275
Why Group Profiles?	276
Implementation	278
Chapter 14: Role-Based Access for IT	281
Security and Your IT Staff	281
Identify the Roles	282
Define a Secure Environment for Each Business Function	282
Operator	282
Network Administrator for IBM i	286
Help Desk	286
Programmer/Analyst	287
System and Security Administrators	290
Security for Vendors and Consultants	291
Vendor Support	291
Consultant Practices	292
Role-Based IT Access	293
Chapter 15: Auditing	295
The History Log	296
History Log Housekeeping	297
Inside Information	298
The Security Audit Journal	298
The Audit Journal	299
Auditing Controls	300
System-Wide Auditing	300
Other Auditing Values	304
User Auditing	306
Object Auditing	307
Object Auditing for New Objects	309
Event-Auditing Recommendations	310
Auditing Controls Security Recommendations	310
System and User Event-Auditing Security Recommendations	310
Object-Auditing Recommendations	311
Working with the Audit Journal	311
Understanding Journal Entry Formats	312
Displaying and Printing Audit Journal Entries	315
Using the DSPAUDJRNE Command to Display Entries	315

Using the DSPJRN Command to Display Entries	316
Using the CPYAUDJRNE Command	318
Reporting on Activities from the Information in the Audit Journal	319
Sending Information to Your SIEM	320
What Is Your SIEM Being Used For?	320
What Should You Send to Your SIEM?	321
What About Other Logs?	323
Using SIEM Wisely	323
Benefits of the IBM i Architecture	324
Helpful Tools	324
Navigator for i	324
Chapter 16: Authority Collection	327
Authority Collection by User	327
Too Much Authority or Determining What Authority Is Required	328
Debugging an Authority Failure	330
Determining the Source of Authority	330
Determining Users' Access to an IFS Object	331
Authority Collection—By Object	333
Determining Who Is Accessing Objects	334
Interpreting the Collection	335
Determining What's Configured	336
Save the Collection	337
SQL Views in QSYS2	338
Chapter 17: Implementing Object-Level Security	339
Determine the Scope of Your Project	339
High-Level Design of the Architecture	341
Building the Big Picture	342
Collecting the Information	344
Dynamic SQL	346
Decision Points	347
Owning All Application Objects Rather Than Being Authorized	347
What Adopts	348
Authorization Lists	349
*PUBLIC Authority	350
How Many Authorization Lists?	350
*PUBLIC Authority	351
*PUBLIC Authority of Programs	351
Securing Libraries	351
*PUBLIC Authority of Other Application Objects	352

Queries	352
Making Changes to the Application	354
Rolling Out the Changes	355
Changes to Change Management	357
When Something Breaks: Debugging and Recovery Techniques	357
Making Sure the Changes “Stick”	358
Gotchas	358
Summary	359
Chapter 18: Security Administration	361
Remove Obsolete Objects	361
System Values	362
User Profiles	362
Managing Authorities	365
Regular Reviews	365
Controlling Who Can Do What	366
Integrated File System (IFS)	367
Stay Current	367
Summary	368
Chapter 19: Maintaining Compliance	369
Evaluating the Key Areas	369
System Values	370
User Profiles	370
Object Authority	372
An Annual Security Assessment	373
Regular Reviews	375
Group Profile Membership and Special Authority Assignments	375
Authorization Lists	376
Policies and Processes	376
Summary	377
Chapter 20: Preparing for the Worst:	
 Creating a Security Incident Response Plan	379
Be Prepared	379
Assembling the Incident Response Team	380
Responding to an Incident	381
Data Preservation	382
Performing the Investigation	382
What Do You Do If You Detect What You Feel Is	
Inappropriate Access?	384

What Do You Have Available if You Don't Have Auditing Enabled or Exit Point Software?.....	385
What If You Find an Active Connection?	385
Be Proactive	386
Saving Security Data.....	386
How Often Should You Save Security Data?.....	386
How Often Should You Save Audit Journal Receivers?	386
Restoring Security Data	387
Order Is Important	387
Security Data Restored with an Object.....	388
Recreating the System After a Breach	388
Chapter 21: Creating a Security Awareness Program.....	391
What Method Do I Use to Communicate?	392
Getting Started.....	393
Chapter 22: Tips for Auditors.....	397
What Is IBM i?	397
IBM i Terminology.....	398
What Should You Be Examining?.....	400
System Values.....	400
User Profile Attributes	401
Authority to Data	403
Commands	404
Job Schedulers	405
TCP/IP Servers.....	405
Dates	406
User Profile Dates.....	406
Files, Programs, and Other Objects	406
What Organizations Miss	407
Reviewing Configuration Settings	407
Removing Inactive Profiles.....	407
Saving Security Information	408
Saving Audit Journal Receivers.....	408
Don't Be Fooled	408
Restrictions on System Administrators.....	408
Password Expiration	409
Commands Allowed by a Limited User.....	409
Auditing Essentials.....	409
Index	411

