Contents

Acknowledgements **v**

Introduction **vii**

Chapter 1: Technology Overview **1**

IBM i Access Client Solutions 1

New Navigator for i 4

IBM i Services 4

Authority Collection 5

IBM i Audit Journal 5

Chapter 2: System Values **7**

QSECURITY 7

QSYS2.SECURITY_INFO 9

New Nav: Security Information 10

New Nav: System Values 11

Using the Audit Journal to Detect System Value Changes 13

Chapter 3: Moving to a Higher Security Level **15**

Moving from QSECURITY Level 30 to 40 15

Audit to Determine Whether There Are Issues Prior to Moving to Level 40 16

Domain Failures 17

User Profiles Specified in a Job Description 18

Moving from QSECURITY Level 20 to 40 19

Analyzing and Adjusting Profiles' User Class 20

Determine the Users' Source of Authority to Application Data after IPLing 22

Chapter 4: Moving to a Higher Password Level **25**

QPWDLVLs 0 and 1 25

The Benefits of Moving to QPWDLVL 2 Then 3 26

Changes That Occur with QPWDLVL 2 or 3 27

Moving to QPWDLVL 2 Then 3 31

QPWDLVL 4 33

Chapter 5: User Profiles **35**

Analyzing User Profiles 36

Basic Information 36

Special Authorities 36

Limited Capabilities 38

Inactive Profiles 38

Disabling Inactive Profiles 39

Profiles with a Default Password 39

Analyzing Group Profiles 40

Members of a Group Profile 41

Group Profile Configuration 41

Group Profiles Without Members 42

Other Profiles and Services to Consider 42

Service Accounts 42

Owned Objects 43

User Profile Changes in IBM i 7.5 44

Users and Groups in New Nav 46

User Profiles and the Audit Journal 48

Creation of Profiles with a Special Authority 48

Examining the Audit Journal Using New Nav 50

Chapter 6: Using Authority Collection to Reduce Users' Authority **53**

Authority Collection for Users: Objects in Libraries 54

Authority Collection for Users: Objects in the IFS 58

Authority Collection in New Nav 60

Using Authority Collection to Prepare to Move Off of QSECURITY 20 61

Authority Failure Occurs 61

Which Profiles Have a Collection or Are Actively Collecting? 62

Final Guidance 63

Chapter 7: Object Authorities 65
Object Authorities: IBM i Services for Objects in Libraries 65
Object Authorities: IBM i Services for Objects in Directories 66
Managing Permissions Using IBM i Access Client Solutions (ACS) 67
Authorization Lists: IBM i Services 69
Authorization Lists: New Nav 70
Object Statistics: Objects in Libraries 71
Object Statistics: Objects in Directories 72
Object Statistics: Last_used_object Field 73
Protect Information from Appearing in the Plan Cache and Database Monitors 74
Using the Audit Journal 74
Authority Failure (AF) 74
Options for Getting Entries out of the Audit Journal 75
Insufficient Special Authority 76
Other Audit Journal Types 77
Ownership Changes (OW) 77
Authority Changes (CA) 78
Creation of Objects (CO) 79
Deletion of Objects (DO) 80
More Information 81

Chapter 8: Adopted Authority 83
Discovering Programs That Adopt a Powerful Profile 83
Application Programs 85
Dynamic SQL 86
SQL Naming Conventions and Adopted Authority 87

Chapter 9: Successfully Securing Objects by Using Authority Collection, IBM i Services, and Auditing 89
Reducing Access to a Directory 90
Securing the Directory 92
Reducing Access to a Database File 93
Application Access 95
Other Access 96
Reworking the Authority Scheme of an Entire Application 96
Determining Where Authority Is Coming From 99
Which Objects Have Authority Collection Configured? 101

Chapter 10: Tips for Securing the IFS and Avoiding Malware 103

IFS Authorities 104

File Shares 105

Steps to Reducing the Risk 106

Step #1: Examine who is using the file shares and eliminate ones that are no longer in use. 106

Shares to Root ('/') 110

Step #2: Reduce Read/Write shares to Read-only where possible. 111

Step #3: Set the appropriate permissions to IBM-supplied directories. 112

IBM i NetServer Settings 114

Checking for Announcements 115

Checking for a Guest Profile 116

Reducing the Risk: Exported Mountpoints 117

Reducing the Risk with IBM i 7.5 Enhancements 117

Control Access to the NetServer 117

Control Access to a Specific File Share 119

Final Recommendations for Reducing Risk in the IFS: 121

A Green-Screen Method to Manage NetServer Security 122

Chapter 11: Implementing Function Usage (Application Administration) 123

Controlling Access to New Nav 124

Controlling Access to ACS Features 128

Controlling Access to IBM i Features 128

Listing the Function ID Settings 130

Using the Audit Journal to Detect Access 130

You Need to Do More Than Just Control New Nav and ACS to Secure Your Data 131

Chapter 12: Securing the Connection to IBM i 133

TCP/IP Servers 133

Exit Points 134

Controlling Who Can Use SSH 136

Other Best-Practice Settings 138

Discovering Who's Using SSH 139

SNMP 140

Encrypted Sessions 140

Ensuring All Communications Are Encrypted 141

NETSTAT 142

The Audit Journal 142

Helpful Hints 144

Ensure All Connections Are Using Strong Encryption 145

Securing New Nav 147

Chapter 13: Automating Your Analysis 149

Run SQL Scripts 149

SQL in a CL Program 149

Using Administration Runtime Expert (ARE) 151

Chapter 14: A Little Bit of Everything 157

Other IBM i 7.5 Enhancements to Be Aware Of 157

Table Functions That Help Keep Your System Current 159

Using the Integrated Security Tools: SECTOOLS 160

Reducing the Time of Your SAVSECDTA 164

What's Saved When You Run Save Security Data (SAVSECDTA)? 164

The Value of Saving Time 168

The Audit Journal as an Early Warning System 168