

CONTENTS

Acknowledgments.....	v
Dedication.....	vii
Author Biography.....	ix
About the Technical Editor.....	xi
Introduction.....	xxi

CHAPTER 1 Securing the Network.....	1
Securing the Network.....	1
Network Firewalls.....	2
Server Firewalls.....	7
Direct Internet Access.....	9
Public IP Addresses versus Private IP Addresses.....	11
Accessing SQL Server from Home.....	14
Physical Security.....	15
Keep Your Hands Off My Box.....	16
Open Network Ports.....	17
Unlocked Workstations.....	17
Social Engineering.....	20
Finding the Instances.....	20
Testing the Network Security.....	22
Summary.....	24

CHAPTER 2 Database Encryption.....	25
Database Encryption.....	25
Hashing versus Encryption.....	25
Hashing.....	27
Encrypting Objects.....	29
Encrypting Data within Tables.....	30
Encrypting within Microsoft SQL Server.....	32
Encrypting Data at Rest.....	41
TDE and FILESTREAM.....	44
Log Shipping, Database Mirroring, and Always On.....	44
Key Protection.....	45
Encrypting Data on the Wire.....	46
SQL Server Over SSL.....	46
Hiding the Instance.....	54
IP Sec.....	54

Encrypting Data with MPIO Drivers	60
PowerPath Encryption with RSA	
Requirements and Setup	62
Encrypting Data via HBAs	72
Summary	73
CHAPTER 3 SQL Password Security	75
SQL Server Password Security	75
Extended Protection	77
Strong Passwords	81
Contained Database Logins in SQL Server 2012	84
Encrypting Client Connection Strings	88
SQL Reporting Services	88
Application Roles	89
Using Windows Domain Policies to Enforce	
Password Length	93
Windows Authentication Group Policies	95
Windows Domain Requirements to Use Domain	
Policies to Manage SQL Authentication Logins	97
Contained Databases	100
Contained Databases and Auto Close	100
db_owners Can Now Add New Users to the	
Instance	100
Password Policies and Contained Users	101
Summary	101
CHAPTER 4 Securing the Instance	103
What to Install, and When?	103
SQL Authentication and Windows Authentication	106
Editing the master.mdf File	110
Using a Debugger to Intercept Passwords	111
Purchased Products	111
Password Change Policies	111
Auditing Failed Logins	114
Renaming the SA Account	115
Disabling the SA Account	116
Securing Endpoints	118
Stored Procedures as a Security Measure	119
Access to Base Tables Isn't Required	120
Minimum Permissions Possible	121
Instant File Initialization	123

Linked Servers	125
NTLM Double Hop Problems	126
Securing Linked Servers.....	126
Using Policies to Secure Your Instance	132
SQL Azure Specific Settings	137
Instances That Leave the Office.....	138
Securing “Always On”.....	140
Securing Contained Databases	141
Contained Databases and Always On.....	144
Summary	144
CHAPTER 5 Additional Security for an Internet Facing SQL Server and Application	147
SQL CLR	147
Extended Stored Procedures	152
Protecting Your Connection Strings.....	154
Database Firewalls	155
Clear Virtual Memory Pagefile	155
User Access Control (UAC).....	159
Other Domain Policies to Adjust	162
Summary.....	163
CHAPTER 6 Analysis Services	165
Logging into Analysis Services	165
Granting Administrative Rights	166
Granting Rights to an Analysis Services Database.....	168
Securing Analysis Services Objects.....	172
Data Sources	172
Cubes	174
Cell Data.....	177
Dimensions	179
Dimension Data	181
Mining Structures	185
Summary.....	190
CHAPTER 7 Reporting Services	191
Setting up SSRS.....	191
Service Account	194
Web Service URL.....	195
Database	197
Report Manager URL.....	200

E-mail Settings	200
Execution Account.....	202
Encryption Keys	202
Scale-Out Deployment	204
Logging onto SQL Server Reporting Services for the first time.....	205
Security within Reporting Services	206
Item Roles.....	206
System Roles	208
Adding System Roles	209
Adding Folder Roles.....	211
Reporting Services Authentication Options.....	213
Anonymous Authentication	214
Forms Authentication	216
Security Within Reporting Services	217
Report Server Object Rights.....	218
Changing Permissions on an Object.....	218
Hiding Objects.....	220
Summary.....	220
CHAPTER 8 SQL Injection Attacks	221
What is an SQL Injection Attack?	221
Why are SQL Injection Attacks so Successful?	226
How to Protect Yourself From an SQL Injection Attack.....	227
NET Protection Against SQL Injection	227
Protecting Dynamic SQL Within Stored Procedures from SQL Injection Attack.....	232
Using “EXECUTE AS” to Protect Dynamic SQL	233
Removing Extended Stored Procedures	236
Not Using Best Practice Code Logic can Hurt You.....	236
What to Return to the End User	238
Database Firewalls.....	239
Test, Test, Test	240
Cleaning Up the Database After an SQL Injection Attack	240
Other Front-End Security Issues.....	243
The Web Browser URL is Not the Place for Sensitive Data.....	243
Using xEvents to Monitor For SQL Injection	245
Summary	247

CHAPTER 9 Database Backup Security	249
Overwriting Backups	250
Deleting Old Backups.....	252
Media Set and Backup Set Passwords	255
Backup Encryption	256
LiteSpeed for SQL Server	257
Red Gate SQL HyperBac	257
Red Gate SQL Backup	258
Third-Party Tape Backup Solutions.....	259
Transparent Data Encryption.....	260
Securing the Certificates.....	261
Compression and Encryption.....	262
Encryption and Data Deduplication	263
Offsite Backups.....	264
Summary.....	266
CHAPTER 10 Storage Area Network Security	267
Securing the Array	267
Locking Down the Management Ports	268
Authentication	269
User Access to the Storage Array	270
Locking Down the iSCSI Ports	270
LUN Security.....	270
Snapshots and Clones	271
Securing the Storage Switches.....	272
Fiber Channel	272
iSCSI.....	273
Fiber Channel over Ethernet.....	273
Management Ports	273
Authentication	274
Zone Mapping	274
Summary.....	274
CHAPTER 11 Auditing for Security	275
Login Auditing.....	276
SQL Server 2005 and Older	276
SQL Server 2008 and Newer.....	278
Using xEvents for Auditing Logins.....	284
Auditing sysadmin Domain Group Membership	289
Data Modification Auditing	290
Change Data Capture Configuration	291

Querying Changed Data	293
Using xEvents For Data Modification Auditing	294
Using SQL Server Audit for Data Modification	296
Data Querying Auditing.....	297
Schema Change Auditing	300
Using Extended Events for Schema Change Auditing	300
Using Policy-Based Management to Ensure Policy Compliance	302
C2 Auditing.....	306
Common Criteria Compliance.....	308
Summary.....	310
CHAPTER 12 Server Rights	311
SQL Server Service Account Configuration.....	312
One Account for All Services	312
One Account Per Sever	313
One Account for Each Service	313
Using Local Service Accounts for Running SQL Server Services	314
Credentials	317
SQL Server Agent Proxy Accounts	320
OS Rights Needed by the SQL Server Service.....	323
Windows System Rights	323
SQL Server's NTFS Permissions	325
OS Rights Needed by the DBA	325
Dual Accounts	326
OS Rights Needed to Install Service Packs	327
OS Rights Needed to Access SSIS Remotely.....	327
Console Apps must die	330
Fixed-Server Roles	331
User Defined Server Roles.....	332
AlwaysOn	333
Instance Wide Permissions	334
Fixed Database Roles.....	334
Fixed Database Roles in the msdb Database	335
User Defined Database Roles	337
Default Sysadmin Rights	339
Vendor's and the Sysadmin Fixed-Server Role	340
Summary.....	341

CHAPTER 13 Securing Data	343
GRANTing Rights	344
DENYing Rights.....	348
REVOKEing Rights.....	349
Column Level Permissions	349
Row Level Permissions.....	351
Summary	354
Appendix	355
Index	367