Contents at a Glance

Part I **Understanding Your Security Culture**

Chapter 1 **Information Security: Adventures in Culture Hacking** 3

Chapter 2 **Strategy for Breakfast: The Hidden Power of Security Culture** 19

Chapter 3 **Organizational Culture: A Primer** 39

Chapter 4 **Cultural Threats and Risks** 59

Part II **Measuring Your Security Culture**

Chapter 5 **The Competing Security Cultures Framework** 81

Chapter 6 **The Security Culture Diagnostic Survey (SCDS)** 115

Chapter 7 **Creating Culture Maps with the Security Culture Diagnostic Survey** . . . 139

Chapter 8 **Implementing a Successful Security Culture Diagnostic Project** 159

Part III **Transforming Your Security Culture**

Chapter 9 **From Diagnosis to Transformation: Implementing People-Centric Security** 189

Chapter 10 **Security FORCE: A Behavioral Model for People-Centric Security** 201

Chapter 11 **The Security Value of Failure** 219

Chapter 12 **The Security Value of Operations** 239

Chapter 13 **The Security Value of Resilience** 263

Chapter 14 **The Security Value of Complexity** 285

Chapter 15 **The Security Value of Expertise** 309

Chapter 16 **Behavior and Culture: Mastering People-Centric Security** 333

Chapter 17 **Leadership, Power, and Influence in People-Centric Security** 357

Chapter 18 **Securing a People-Centric Future** 369

Index 381

Contents

Foreword xvii
Acknowledgments xviii
Introduction xix

Part I **Understanding Your Security Culture**

Chapter 1 **Information Security: Adventures in Culture Hacking** **3**
Burnt Bacon 4
Safe and Not Secure 6
What Were You Thinking? 6
Culture Hacking 7
Software of the Mind 8
A Brief History of Culture Hacking 9
Security Culture: Hack or Be Hacked 10
Who's Hacking Your Security Culture? 11
Security, Hack Thyself 12
Culture Hacks: The Good 14
Culture Hacks: The Bad 15
Culture Hacks: The Ugly 16
Security Is People! 17
Further Reading 17

Chapter 2 **Strategy for Breakfast: The Hidden Power of Security Culture** **19**
Why Security Fails 20
We Start with a Design 20
Warning Signs 22
Doing More with Less 23
Who Moved My Fence? 24
Look Out Below! 27
Getting the Drift 27

The Opposite of Monoculture . . . 28
Cultural Traits in Information Security . . . 30
Competing Values and Security Threats . . . 34
The Change Agents of Security Culture . . . 35
The C-Suite . . . 35
Security Awareness Teams . . . 36
Security Researchers . . . 36
Security Practitioners . . . 37
Making Security Cultural . . . 38
Further Reading . . . 38

Chapter 3 **Organizational Culture: A Primer** . . . **39**
The Field of Organizational Culture . . . 41
Origins . . . 41
Outcomes . . . 42
The Culture Iceberg . . . 43
Hidden Aspects . . . 44
People Powered . . . 46
The Organizational Cultural/Organizational Performance Link . . . 47
Assessing and Measuring Culture . . . 49
Qualitative vs. Quantitative Measurement of Culture . . . 49
Qualitative Measures and Techniques . . . 50
Culture by the Numbers . . . 51
Challenges of Cultural Transformation . . . 53
There's No One Right Way to Change Culture . . . 54
You Have to Include Everybody . . . 54
You Have to Build Consensus . . . 54
You Have to Evaluate the Outcomes . . . 55
You Have to Have Good Leadership . . . 56
An Ocean of Research . . . 57
Further Reading . . . 57

Chapter 4 **Cultural Threats and Risks** . . . **59**
Cultural Threat Modeling . . . 60
Covert Processes and Cultural Risk . . . 61
Getting to Know PEPL . . . 62
Political Threats . . . 64
Emotional Threats . . . 66

Psychological Threats 68
Logistical Threats 72
Cultural Competition as a Source of Risk 73
Sizing Up the Competition 74
Further Reading 77

Part II **Measuring Your Security Culture**

Chapter 5 **The Competing Security Cultures Framework 81**
Measuring Security Culture 82
Quantitative Data and Analysis 83
Qualitative Data and Analysis 87
Combining the Qualitative and Quantitative 88
Other Ways of Describing Culture 91
The Competing Security Cultures Framework 94
Origins of the CSCF in Competing Values Research 94
Adapting the Competing Values Framework to Security 96
The CSCF Quadrants 99
Overlapping and Competing Values 100
Limitations of the Framework 101
Why Not Just Use the Competing Values Framework? 102
Security Culture Benefits From a Targeted Approach 102
Not Everything in the Competing Values Framework Translates Well 103
Organizational Security Cultures 104
Process Culture 104
Compliance Culture 106
Autonomy Culture 109
Trust Culture 112
Further Reading 114

Chapter 6 **The Security Culture Diagnostic Survey (SCDS) 115**
SCDS Format and Structure 117
How Surveys Work 117
Questions in the SCDS 118
SCDS Scoring Methodology 125
Scoring the SCDS Results 126

Security Culture Diagnostic Strategies: Case Studies 128
ABLE Manufacturing: Measuring an Existing Security Culture 128
CHARLIE Systems, Inc.: Comparing Security Cultures of Two Organizations 133
DOG: Comparing Existing to Desired Security Culture 135

Chapter 7 **Creating Culture Maps with the Security Culture Diagnostic Survey . . . 139**
Security Culture Maps 141
Mapping Security Culture Using the CSCF 141
Composition of a SCDS-based Culture Map 143
Other Techniques for Mapping Security Culture 146
"When Should I Use Each Type of Map?" 148
Mapping Specific Values and Activities 149
Interpreting and Comparing Culture 150
Interpreting SCDS Results 151
Comparing Cultures 156

Chapter 8 **Implementing a Successful Security Culture Diagnostic Project 159**
Getting Buy-in for the Security Culture Diagnostic Project 160
Direct Benefits of Security Culture Improvement 160
Estimating the Financial Impact of Security Culture 162
Case Study: FOXTROT Integrators, Inc. 164
Executing a Security Culture Diagnostic Project 170
1. Setting Up the Project 171
2. Collecting Data 175
3. Analyzing Responses 180
4. Interpreting Culture and Communicating Results 181
From Measurement to Transformation 185
Further Reading 185

Part III Transforming Your Security Culture

Chapter 9 **From Diagnosis to Transformation: Implementing People-Centric Security 189**
Diagnosis and Transformation: One Coin, Two Sides 190
The CSCF as a Framework for Understanding 190
What Is the Framework for Transformation? 191
Behavioral Models for Security Culture Transformation 192
Compliance and Control Regimes 192
Security Process Improvement 194

Technology and Automation Approaches 196
Security Needs More Options 198
Further Reading 199

Chapter 10 **Security FORCE: A Behavioral Model for People-Centric Security 201**
Origins of Security FORCE 203
HRO Research 204
HROs in Information Security 206
Introducing the Security FORCE Behavioral Model 208
Five Core Values of Security FORCE 209
Security FORCE Value Behaviors and Metrics 211
Security FORCE Value Behaviors 212
Security FORCE Value Metrics 212
The Culture–Behavior Link in HRSPs 215
Further Reading 217

Chapter 11 **The Security Value of Failure 219**
What Is the Security Value of Failure? 220
"Failure Is Not an Option" 220
Reevaluating Failure 221
Embracing Failure 223
Fail Small, Fail Fast, Fail Often 224
Failure Key Value Behaviors 226
Anticipate Failures 227
Seek Out Problems 227
Reward Problem Reporting 228
Share Information About Failures 229
Learn from Mistakes 230
Assessing Your Failure Value Behaviors 232
The Security FORCE Survey 232
The Security FORCE Metrics 234
Improving Your Failure Value Behaviors 237
Embed the Security Value of Failure into People 237
Reeducate People on What It Means to Fail 237
Set Leadership Examples 238
Open Up Communication 238
Further Reading 238

Chapter 12 **The Security Value of Operations** **239**
What Is the Security Value of Operations? 240
Operational Power 241
Sensitivity to Operations 241
Expectations and Reality 243
Operations Key Value Behaviors 244
Keep Your Eyes Open 245
Form a Bigger Picture 246
"Listen" to the System 247
Test Expectations Against Reality 249
Share Operational Assessments 252
Assessing Your Operations Value Behaviors 255
Scoring the Operations Value Behavior Survey 255
FORCE Value Metrics for Operations 256
Improving Your Operations Value Behaviors 259
Embed Operations Value into the Security Program 259
Think More Like Scientists 260
Embrace the "Sharing Economy" 260
Lighten Up a Bit 261
Further Reading 261

Chapter 13 **The Security Value of Resilience** **263**
What Is the Security Value of Resilience? 264
When Bad Things Happen (to Good Organizations) 264
Rolling with the Punches 266
Imagining Failures and Disasters 267
Resilience Key Value Behaviors 270
Overtrain People 270
Create "Skill Benches" 272
Actively Share Expertise 273
Encourage Stretch Goals 274
Practice Failing 275
Assessing Your Resilience Value Behaviors 278
Scoring the Resilience Value Behavior Survey 278
FORCE Value Metrics for Resilience 279

Improving Your Resilience Value Behaviors 281
Embed Resilience Value into the Security Program 282
"A Security Incident? I Want In!" 282
Make Security Incidents Mundane 283
Further Reading 283

Chapter 14 **The Security Value of Complexity 285**
What Is the Security Value of Complexity? 286
Dumbing It Down 287
Growing Uncertainty 288
Ignorance Is Risk 290
Complexity Key Value Behaviors 294
Don't Oversimplify 295
Formalize Your Assumptions 296
Covet Empirical Evidence 297
Share the Doubt 298
Make Every Model Better 299
Assessing Your Complexity Value Behaviors 300
Scoring the Complexity Value Behavior Survey 301
FORCE Value Metrics for Complexity 302
Improving Your Complexity Value Behaviors 304
Embed Complexity Value into the Security Program 305
Think Bigger 306
Accept What We Already Know 306
Further Reading 307

Chapter 15 **The Security Value of Expertise 309**
What Is the Security Value of Expertise? 311
Filter Your Water, Not Your Information 311
Structural Authority vs. Structural Knowledge 312
Waiting for the Big One 315
Expertise Key Value Behaviors 317
Ask the Experts 318
Suppress the Egos 319
Allow Authority to Migrate 320
Share Credibility 321
Reward Calls to Action and Cries for Help 322

Assessing Your Expertise Value Behaviors 324
Scoring the Expertise Value Behavior Survey 325
FORCE Value Metrics for Expertise 326
Improving Your Expertise Value Behaviors 328
Embed Expertise Value into the Security Program 329
Make Everyone a Sensor 329
Create Decision Fast Lanes 330
Value Expertise from the Top Down 331
Further Reading 331

Chapter 16 **Behavior and Culture: Mastering People-Centric Security 333**
What Does Security Culture Transformation Mean? 334
Describing Transformation in Terms of Cultural Capabilities Maturity 334
The Cultural Capabilities Maturity Model: Formalizing Cultural Maturity 335
Supporting Security Culture Transformation with Security FORCE Projects 338
The Value of a Security FORCE Project 338
Managing a Security FORCE Project 338
The Security FORCE Scorecard 340
Scoring the FORCE Survey Questions, Revisited 341
Pooling Your FORCEs 341
Security FORCE Metrics and the FORCE Scorecard 342
"Are We a Highly Reliable Security Program?" 343
CSCF and Security FORCE: Aligning Culture and Behavior in People-Centric Security 347
Chaining Culture and Behavior Efforts 348
Using the SCDS and FORCE Independently 349
General Alignments Between Security FORCE and the CSCF 349
Taking Advantage of Cultural-Behavioral Alignments 353
Blending Security Culture Diagnostic and Security FORCE Projects for Improved Cultural Maturity 355
Further Reading 356

Chapter 17 **Leadership, Power, and Influence in People-Centric Security 357**
A Crisis of Leadership 358
The CISO as a Business Leader 359
Business Leaders as Security Enablers 360
Security Power Dynamics 361
"What if I am not a CISO?" 362

Leadership in People-Centric Security 364
You Don't Lead Machines 364
Influence and Transformation 365
Adapting the CSCF and Security FORCE Model to Leadership 365
The CSCF, SCDS, and Cultural Leadership 366
The Security FORCE Model and Behavioral Leadership 367
Further Reading 367

Chapter 18 **Securing a People-Centric Future 369**
The Security of Things 370
Social Security 371
As Many Securities as Things to Secure 371
Framing People-Centric Security 375
Security Soft Power 375
Three Takeaways from the Book 376
Putting People-Centric Security to Work 377
Two Models, One Goal 377
People-Centric Security Strategies 378
Conclusion 379
Further Reading 380

Index 381