



At a Glance

PART I **Introducing Security Metrics**

1	What Is a Security Metric?	3
2	Designing Effective Security Metrics	25
3	Understanding Data	55
	Case Study 1: In Search of Enterprise Metrics	73

Part II **Implementing Security Metrics**

4	The Security Process Management Framework	89
5	Analyzing Security Metrics Data	111
6	Designing the Security Measurement Project	151
	Case Study 2: Normalizing Tool Data in a Security Posture Assessment	171

PART III Exploring Security Measurement Projects

7	Measuring Security Operations	195
8	Measuring Compliance and Conformance ...	223
9	Measuring Security Cost and Value	247
10	Measuring People, Organizations, and Culture	271
	Case Study 3: Web Application Vulnerabilities	289

PART IV Beyond Security Metrics

11	The Security Improvement Program	307
12	Learning Security: Different Contexts for Security Process Management	329
	Case Study 4: Getting Management Buy-in for the Security Metrics Program	339
	Index	357

Contents

Foreword	xix
Acknowledgments	xxi
Introduction	xxiii

Part I

Introducing Security Metrics

1 What Is a Security Metric?	3
Metrics and Measurement	5
Metrics Are a Result	6
Measurement Is an Activity	6
Security Metrics Today	8
Risk	8
Security Vulnerability and Incident Statistics	14
Annualized Loss Expectancy	15
Return on Investment	17
Total Cost of Ownership	18
The Dissatisfying State of Security Metrics:	
Lessons from Other Industries	19
Insurance	19
Manufacturing	20
Design	21

Reassessing Our Ideas About Security Metrics	22
Thinking Locally	22
Thinking Analytically	23
Thinking Ahead	23
Summary	23
Further Reading	24
2 Designing Effective Security Metrics	25
Choosing Good Metrics	26
Defining Metrics and Measurement	27
Nothing Either Good or Bad, but Thinking Makes It So	28
What Do You Want to Know?	32
Observe!	35
GQM for Better Security Metrics	36
What Is GQM?	36
Setting Goals	38
Asking Questions	42
Assigning Metrics	43
Putting It All Together	45
The Metrics Catalog	45
More Security Uses for GQM	47
Measuring Security Operations	47
Measuring Compliance to a Regulation or Standard	48
Measuring People and Culture	50
Applying GQM to Your Own Security Measurements	52
Summary	52
Further Reading	53
3 Understanding Data	55
What Are Data?	56
Definitions of Data	57
Data Types	58
Data Sources for Security Metrics	68
System Data	68
Process Data	69
Documentary Data	69
People Data	70
We Have Metrics and Data—Now What?	71
Summary	72
Further Reading	72

Case Study 1: In Search of Enterprise Metrics	73
Scenario One: Our New Vulnerability Management Program . . .	77
Scenario Two: Who's on First?	78
Scenario Three: The Value of a Slide	79
Scenario Four: The Monitoring Program	82
Scenario Five: What Cost, the Truth?	84
Summary	86

Part II

Implementing Security Metrics

4 The Security Process Management Framework	89
Managing Security as a Business Process	90
Defining a Business Process	91
Security Processes	92
Process Management over Time	93
The SPM Framework	96
Security Metrics	98
Security Measurement Projects	98
The Security Improvement Program	100
Security Process Management	101
Before You Begin SPM	103
Getting Buy-in: Where's the Forest?	103
The Security Research Program	108
Summary	109
Further Reading	110
5 Analyzing Security Metrics Data	111
The Most Important Step	112
Reasons for Analysis	113
What Do You Want to Accomplish?	116
Preparing for Data Analysis	116
Analysis Tools and Techniques	121
Descriptive Statistics	122
Inferential Statistics	130
Other Statistical Techniques	135
Qualitative and Mixed Method Analysis	140
Summary	147
Further Reading	149

6 Designing the Security Measurement Project	151
Before the Project Begins	152
Project Prerequisites	153
Deciding on a Project Type	154
Tying Projects Together	156
Getting Buy-in and Resources	156
Phase One: Build a Project Plan and Assemble the Team	160
The Project Plan	160
The Project Team	161
Phase Two: Gather the Metrics Data	163
Collecting Metrics Data	163
Storing and Protecting Metrics Data	164
Phase Three: Analyze the Metrics Data and Build Conclusions ..	164
Phase Four: Present the Results	166
Textual Presentations	167
Visual Presentations	167
Disseminating the Results	168
Phase Five: Reuse the Results	168
Project Management Tools	169
Summary	170
Further Reading	170
Case Study 2: Normalizing Tool Data in a Security	
Posture Assessment	171
Background: Overview of the SPA Service	172
SPA Tools	175
Data Structures	175
Objectives of the Case Study	176
Methodology	177
Challenges	177
Summary	191

PART III

Exploring Security Measurement Projects

7 Measuring Security Operations	195
Sample Metrics for Security Operations	196
Sample Measurement Projects for Security Operations	198
SMP: General Risk Assessment	198
SMP: Internal Vulnerability Assessment	208
SMP: Inferential Analysis	215
Summary	221
Further Reading	221

8 Measuring Compliance and Conformance	223
The Challenges of Measuring Compliance	224
Confusion Among Related Standards	224
Auditing or Measuring?	226
Confusion Across Multiple Frameworks	227
Sample Measurement Projects for Compliance and Conformance	228
Creating a Rationalized Common Control Framework	228
Mapping Assessments to Compliance Frameworks	236
Analyzing the Readability of Security Policy Documents ...	238
Summary	245
Further Reading	245
 9 Measuring Security Cost and Value	 247
Sample Measurement Projects for Compliance and Conformance	248
Measuring the Likelihood of Reported Personally Identifiable Information (PII) Disclosures	248
Measuring the Cost Benefits of Outsourcing a Security Incident Monitoring Process	254
Measuring the Cost of Security Processes	261
The Importance of Data to Measuring Cost and Value	268
Summary	268
Further Reading	269
 10 Measuring People, Organizations, and Culture	 271
Sample Measurement Projects for People, Organizations, and Culture	273
Measuring the Security Orientation of Company Stakeholders	273
An Ethnography of Physical Security Practices	280
Summary	287
Further Reading	288
 Case Study 3: Web Application Vulnerabilities	 289
Source Data and Normalization	291
Outcomes, Timelines, Resources	291
Initial Reporting with “Dirty Data”	292
Ambiguous Data	293
Determining Which Source to Use	293
Working with Stakeholders to Perform Data Cleansing	296

Follow-up with Reports and Discussions with Stakeholders . . .	297
Lesson Learned: Fix the Process, and Then Automate	298
Lesson Learned: Don't Wait for Perfect Data Before Reporting . . .	301
Summary	302

PART IV

Beyond Security Metrics

11 The Security Improvement Program	307
Moving from Projects to Programs	308
Managing Security Measurement with a Security Improvement Program	309
Governance of Security Measurement	311
The SIP: It's Still about the Data	312
Requirements for a SIP	314
Before You Begin	314
Documenting Your Security Measurement Projects	317
Sharing Your Security Measurement Results	318
Collaborating Across Projects and Over Time	319
Measuring the SIP	321
Security Improvement Is Habit Forming	321
Is the SIP Working?	322
Is Security Improving?	322
Case Study: A SIP for Insider Threat Measurement	323
Summary	327
Further Reading	328
12 Learning Security: Different Contexts for Security Process Management	329
Organizational Learning	330
Three Learning Styles for IT Security Metrics	331
Standardized Testing: Measurement in ISO/IEC 27004	332
The School of Life: Basili's Experience Factory	333
Mindfulness: Karl Weick and the High-Reliability Organization	335
Final Thoughts	336
Summary	337
Further Reading	337

Case Study 4: Getting Management Buy-in for the Security Metrics Program 339

The CISO Hacked My Computer 341

What Is Buy-in? 342

Corporations vs. Higher Ed: Who’s Crazy? 343

Higher Education Case Study 343

 Project Overview 344

 Themes 344

 Findings 349

 Key Points 352

 Influence and Organizational Change 353

Conclusion 355

Index 357