

Contents

	Foreword	xv
	Preface	xix
	Acknowledgments	xxv
	About the Author	xxviii
Chapter 1	Introduction: Escaping the Hamster Wheel of Pain	1
	Risk Management Is Where the Confusion Is	1
	Metrics Supplant Risk Management	5
	Summary	7
Chapter 2	Defining Security Metrics	9
	Security Measurement Business Drivers	11
	Roadblocks to Data Sharing	12
	Modeling Security Metrics	13
	Modelers Versus Measurers	13
	Quality Assurance Literature	15
	Public Health Terminology and Reporting Structure	16
	Portfolio Management	17
	Accelerated Failure Testing	17
	Insurance	18
	What Makes a Good Metric?	19
	“Metric” Defined	21
	Consistently Measured	23
	Cheap to Gather	23

Expressed as a Number or Percentage	24
Expressed Using at Least One Unit of Measure	25
Contextually Specific	25
What Makes a Bad Metric?	26
Inconsistently Measured	26
Cannot Be Gathered Cheaply	27
Does Not Express Results with Cardinal Numbers and Units of Measure	27
What Are Not Metrics?	28
Misuse of Security Taxonomies	28
Annualized Loss Expectancy	31
Summary	36

Chapter 3	Diagnosing Problems and Measuring Technical Security	39
	Using Metrics to Diagnose Problems: A Case Study	41
	Defining Diagnostic Metrics	44
	Perimeter Security and Threats	46
	E-mail	49
	Antivirus and Antispam	50
	Firewall and Network Perimeter	50
	Attacks	51
	Coverage and Control	52
	Antivirus and Antispyware	58
	Patch Management	59
	Host Configuration	62
	Vulnerability Management	65
	Availability and Reliability	68
	Uptime	69
	System Recovery	71
	Change Control	72
	Application Security	73
	Black-Box Defect Metrics	75
	Qualitative Process Metrics and Indices	77
	Code Security Metrics	83
	Summary	87

Chapter 4	Measuring Program Effectiveness	89
	Using COBIT, ITIL, and Security Frameworks	91
	Frameworks	91
	Not Useful: Asset Valuation	95
	Planning and Organization	98
	Assessing Risk	99
	Human Resources	101
	Managing Investments	102
	Acquisition and Implementation	104
	Identifying Solutions	104
	Installing and Accrediting Solutions	107
	Developing and Maintaining Procedures	111
	Delivery and Support	112
	Educating and Training Users	114
	Ensuring System Security	117
	Identifying and Allocating Costs	120
	Managing Data	122
	Managing Third-Party Services	123
	Monitoring	126
	Monitoring the Process	127
	Monitoring and Evaluating Internal Controls	128
	Ensuring Regulatory Compliance	129
	Summary	130
Chapter 5	Analysis Techniques	133
	Mean (Average)	135
	Median	136
	Standard Deviation	137
	Grouping and Aggregation	140
	Records and Attributes	140
	Grouping	142
	Aggregation	143
	Time Series Analysis	145
	Cross-Sectional Analysis	147
	Quartile Analysis	150
	Quartile Summary Statistics	151
	First-Versus-Fourth Analyses	152
	Correlation Matrices	152
	Summary	156

Chapter 6	Visualization	157
	Design Principles	160
	It Is About the Data, Not the Design	161
	Just Say No to Three-Dimensional Graphics and Cutesy Chart Junk	161
	Don't Go off to Meet the Wizard	162
	Erase, Erase, Erase	162
	Reconsider Technicolor	163
	Label Honestly and Without Contortions	164
	Example	165
	Stacked Bar Charts	168
	Waterfall Charts	170
	Time Series Charts	172
	Basic Time Series Charts	172
	Indexed Time Series Charts	174
	Quartile Time Series Charts	175
	Bivariate (X-Y) Charts	177
	Two-Period Bivariate Charts	180
	Small Multiples	181
	Quartile-Plot Small Multiples	183
	Two-by-Two Matrices	185
	Period-Share Chart	188
	Pareto Charts	191
	Tables	194
	Treemaps	196
	Creating Treemaps	199
	Thinking Like a Cannibal: the Case for Redrawing	203
	A Patch Job for Ecora	203
	Reorienting SecurCompass	207
	Managing Threats to Readability	210
	Summary	214
Chapter 7	Automating Metrics Calculations	217
	Automation Benefits	218
	Accuracy	219
	Repeatability	219
	Increased Measurement Frequency	221
	Reliability	222

Transparency	222
Auditability	223
Can We Use (Insert Your Favorite Tool Here) to Automate Metrics?	224
Spreadsheets	224
Business Intelligence Tools	225
Security Event and Incident Management (SIEM) Products	225
Technical Requirements for Automation Software	227
Data Model	230
Threats	232
Exposures	233
Countermeasures	234
Assets	235
Data Sources and Sinks	236
Data Sources	237
Data Sinks	241
Data Interfaces	242
Data Source Interfaces	242
Data Sink (Presentation) Interfaces	243
Metrics Program Management	244
Implementing Metrics Automation: a Case Study	246
Summary	249
Chapter 8	251
Designing Security Scorecards	251
The Elements of Scorecard Style	253
Complete	253
Concise	254
Clear	255
Relevant	255
Transparent	256
The Balanced Scorecard	257
History	259
Composition	260
Flexibility of the Balanced Scorecard	262
Challenges and Benefits of the Balanced Scorecard	262
Creating the Balanced Security Scorecard	264
The Case Against “Security-Centric” Balanced Scorecards	265
The Process of Creating the Balanced Security Scorecard	267
Financial Perspective	268

Customer Perspective	273
Internal Process Perspective	281
Learning and Growth Perspective	287
Organizational Considerations for the Balanced Security Scorecard	293
Cascading Scorecards Build Bridges	293
Balancing Accountability and Acceptance	295
Speeding Acceptance Using Mock-Ups	296
Summary	298
Index	301