

PRAGMATIC Security Metrics

Applying *Metametrics* to Information Security

W. Krag Brotby and Gary Hinson

Preface by M. E. Kabay, PhD, CISSP-ISSMP

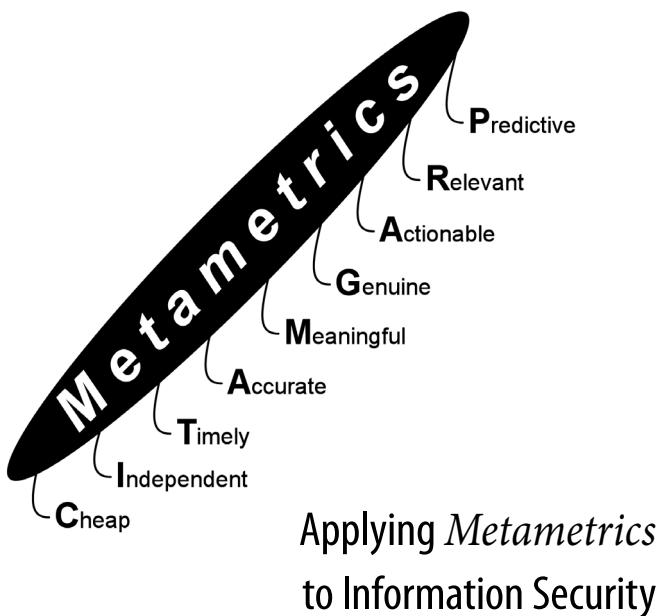


CRC Press
Taylor & Francis Group
AN AUERBACH BOOK

www.ebook777.com

Free ebooks ==> www.ebook777.com

PRAGMATIC Security Metrics



OTHER INFORMATION SECURITY BOOKS FROM AUERBACH

Asset Protection through Security Awareness

Tyler Justin Speed
ISBN 978-1-4398-0982-2

The CISO Handbook: A Practical Guide to Securing Your Company

Michael Gentile, Ron Collette, and Thomas D. August
ISBN 978-0-8493-1952-5

CISO's Guide to Penetration Testing: A Framework to Plan, Manage, and Maximize Benefits

James S. Tiller
ISBN 978-1-4398-8027-2

Cybersecurity: Public Sector Threats and Responses

Kim J. Andreasson, Editor
ISBN 9781-4398-4663-6

Cyber Security Essentials

James Graham, Editor
ISBN 978-1-4398-5123-4

Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS

Tyson Macaulay and Bryan L. Singer
ISBN 978-1-4398-0196-3

Cyberspace and Cybersecurity

George Kostopoulos Request
ISBN 978-1-4665-0133-1

Data Mining Tools for Malware Detection

Mehedy Masud, Latifur Khan, and Bhavani Thuraisingham
ISBN 978-1-4398-5454-9

Defense against the Black Arts: How Hackers Do What They Do and How to Protect against It

Jesse Varsalone and Matthew McFadden
ISBN 978-1-4398-2119-0

Digital Forensics for Handheld Devices

Eamon P. Doherty
ISBN 978-1-4398-9877-2

Electronically Stored Information: The Complete Guide to Management, Understanding, Acquisition, Storage, Search, and Retrieval

David R. Matthews
ISBN 978-1-4398-7726-5

FISMA Principles and Best Practices: Beyond Compliance

Patrick D. Howard
ISBN 978-1-4200-7829-9

Information Security Governance Simplified: From the Boardroom to the Keyboard

Todd Fitzgerald
ISBN 978-1-4398-1163-4

Information Technology Control and Audit, Fourth Edition

Sandra Senft, Frederick Gallegos, and Aleksandra Davis Request
ISBN 978-1-4398-9320-3

Managing the Insider Threat: No Dark Corners

Nick Catrantzos
ISBN 978-1-4398-7292-5

Noiseless Steganography: The Key to Covert Communications

Abdelrahman Desoky
ISBN 978-1-4398-4621-6

Secure and Resilient Software: Requirements, Test Cases, and Testing Methods

Mark S. Merkow
ISBN 978-1-4398-6621-4

Security De-Engineering: Solving the Problems in Information Risk Management

Ian Tibble
ISBN 978-1-4398-6834-8C

The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments, Second Edition

Douglas Landoll
ISBN 978-1-4398-2148-0

The 7 Qualities of Highly Secure Software

Mano Paul
ISBN 978-1-4398-1446-8

Smart Grid Security: An End-to-End View of Security in the New Electrical Grid

Gilbert N. Sorebo and Michael C. Echols
ISBN 978-1-4398-5587-4

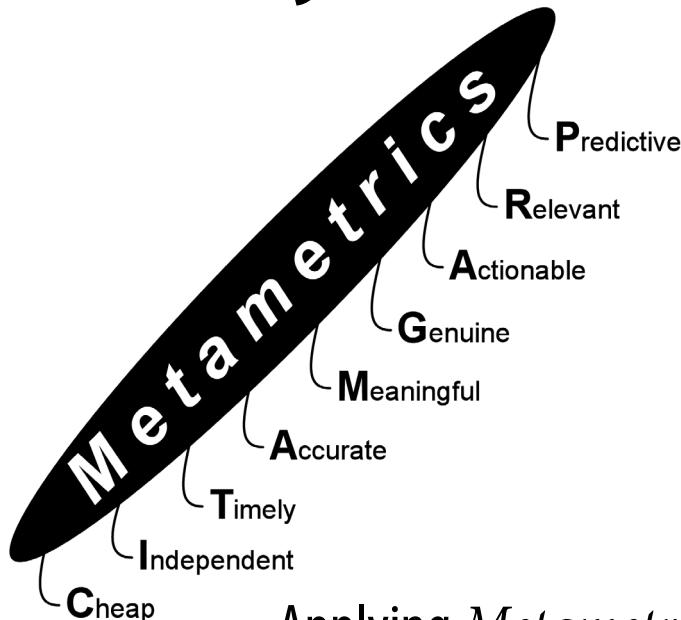
AUERBACH PUBLICATIONS

www.auerbach-publications.com

To Order Call: 1-800-272-7737 • Fax: 1-800-374-3401

E-mail: orders@crcpress.com

PRAGMATIC Security Metrics



Applying *Metametrics*
to Information Security

W. Krag Brotby and Gary Hinson

Preface by M. E. Kabay, PhD, CISSP-ISSMP



CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
AN AUERBACH BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

© 2013 by Taylor & Francis Group, LLC
CRC Press is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works
Version Date: 20121106

International Standard Book Number-13: 978-1-4398-8153-8 (eBook - PDF)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access www.copyright.com (<http://www.copyright.com/>) or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Visit the Taylor & Francis Web site at
<http://www.taylorandfrancis.com>

and the CRC Press Web site at
<http://www.crcpress.com>

Contents

Forewordxi
Preface.....	xiii
Acknowledgments	xv
Office Memorandum	xvii
1 Introduction	1
1.1 Why Have We Written This Book?.....	2
1.2 What's Different about This Metrics Book?	3
1.3 Who Are We Writing This For?.....	5
1.4 Who Are We?	5
1.4.1 W. Krag Brotby	5
1.4.2 Gary Hinson	7
1.5 What We'll Be Talking about.....	8
1.6 Defining Our Terminology	9
1.7 What We Expect of You, the Reader	10
1.8 Summary.....	11
2 Why Measure Information Security?	13
2.1 To Answer Awkward Management Questions.....	15
2.2 To Improve Information Security, Systematically	18
2.3 For Strategic, Tactical, and Operational Reasons.....	20
2.4 For Compliance and Assurance Purposes	22
2.5 To Fill the Vacuum Caused by Our Inability to Measure Security	23
2.6 To Support the Information Security Manager.....	24
2.7 For Profit!	25
2.8 For Various Other Reasons.....	26
2.9 Summary.....	27
3 The Art and Science of Security Metrics.....	29
3.1 Metrology, the Science of Measurement	30
3.2 Governance and Management Metrics	30

vi ■ Contents

3.3	Information Security Metrics	32
3.4	Financial Metrics (for Information Security)	33
3.5	(Information Security) Risk Management Metrics	35
3.6	Software Quality (and Security) Metrics	36
3.7	Information Security Metrics Reference Sources	37
3.7.1	Douglas Hubbard: <i>How to Measure Anything</i> (Hubbard 2010).....	37
3.7.2	Andrew Jaquith: <i>Security Metrics</i> (Jaquith 2007)	38
3.7.3	NIST SP 800-55: <i>Performance Measurement Guide for Information Security</i> (NIST 2008)	39
3.7.4	Debra Herrmann: <i>Complete Guide to Security and Privacy Metrics</i> (Herrmann 2007).....	40
3.7.5	W. Krag Brotby: <i>Information Security Management Metrics</i> (Brotby 2009a)	41
3.7.6	Lance Hayden: <i>IT Security Metrics</i> (Hayden 2010)	41
3.7.7	Caroline Wong: <i>Security Metrics: A Beginner's Guide</i> (Wong 2012)	42
3.7.8	ISO/IEC 27004: <i>Information Security Management– Measurement</i> (ISO/IEC 27004 2009)	42
3.7.9	CIS Security Metrics (CIS 2010)	43
3.7.10	ISACA	44
3.8	Specifying Metrics.....	46
3.9	Metrics Catalogs and a Serious Warning about SMD.....	48
3.10	Other (Information Security) Metrics Resources.....	49
3.11	Summary.....	50
4	Audiences for Security Metrics.....	51
4.1	Metrics Audiences <i>Within</i> the Organization	52
4.1.1	Senior Management.....	53
4.1.2	Middle and Junior Management.....	54
4.1.3	Security Operations.....	55
4.1.4	Others with Interest in Information Security.....	56
4.2	Metrics Audiences From <i>Without</i> the Organization.....	57
4.3	Summary.....	58
5	Finding Candidate Metrics	59
5.1	Preexisting/Current Information Security Metrics	60
5.2	Other Corporate Metrics.....	61
5.3	Metrics Used in Other Fields and Organizations.....	66
5.4	Information Security Metrics Reference Sources	67
5.5	Other Sources of Inspiration for Security Metrics	68
5.5.1	Security Surveys	68
5.5.2	Vendor Reports and White Papers.....	69
5.5.3	Security Software	70

5.6	Roll-Your-Own Metrics	70
5.7	Metrics Supply and Demand	71
5.8	Summary.....	72
6	Metametrics and the PRAGMATIC Approach.....	75
6.1	Metametrics	76
6.2	Selecting Information Security Metrics	78
6.3	PRAGMATIC Criteria.....	81
6.3.1	P = Predictive	82
6.3.2	R = Relevant	85
6.3.3	A = Actionable	86
6.3.4	G = Genuine.....	87
6.3.5	M = Meaningful.....	88
6.3.6	A = Accurate.....	90
6.3.7	T = Timely	91
6.3.8	I = Independent	93
6.3.9	C = Cost.....	94
6.4	Scoring Information Security Metrics against the PRAGMATIC Criteria.....	95
6.5	Other Uses for PRAGMATIC Metametrics	104
6.6	Classifying Information Security Metrics.....	105
6.6.1	<i>Strategic/Managerial/Operational (SMO)</i> Metrics Classification	106
6.6.2	<i>Risk/Control</i> Metrics Classification.....	108
6.6.3	<i>Input–Process–Output (Outcome)</i> Metrics Classification.....	108
6.6.4	<i>Effectiveness and Efficiency</i> Metrics Classification	109
6.6.5	<i>Maturity</i> Metrics Classification.....	109
6.6.6	<i>Directness</i> Metrics Classification	110
6.6.7	<i>Robustness</i> Metrics Classification.....	110
6.6.8	<i>Readiness</i> Metrics Classification	111
6.6.9	<i>Policy/Practice</i> Metrics Classification.....	112
6.7	Summary.....	113
7	150+ Example Security Metrics.....	115
7.1	Information Security Risk Management Example Metrics	118
7.2	Information Security Policy Example Metrics	130
7.3	Security Governance, Management, and Organization Example Metrics.....	140
7.3.1	Information Security Financial Management Metrics	141
7.3.2	Information Security Control-Related Metrics	141
7.3.3	Metrics for Business Alignment and Relevance of Controls.....	142
7.3.4	Control Monitoring and Testing Metrics.....	143
7.3.5	Financial Information Security Metrics	156

viii ■ Contents

7.4	Information Asset Management Example Metrics	160
7.5	Human Resources Security Example Metrics	164
7.6	Physical Security Examples.....	179
7.7	IT Security Metric Examples.....	188
7.8	Access Control Example Metrics	203
7.9	Software Security Example Metrics.....	208
7.10	Incident Management Example Metrics	217
7.11	Business Continuity Management Examples.....	225
7.12	Compliance and Assurance Metrics Examples.....	232
7.13	Summary.....	244
8	Designing PRAGMATIC Security Measurement System	245
8.1	Brief History of Information Security Metrics.....	246
8.2	Taking Systems Approach to Metrics.....	248
8.3	Information Security Measurement System Lifecycle	249
8.4	Summary.....	266
9	Advanced Information Security Metrics	267
9.1	High-Reliability Metrics.....	268
9.2	Indicators and Proxies.....	271
9.3	Key Indicators	272
9.3.1	Key Goal Indicators (KGIs)	272
9.3.2	Key Performance Indicators (KPIs).....	273
9.3.3	Key Risk Indicators (KRIs).....	274
9.3.4	Critical Success Factors (CSFs)	275
9.4	Targets, Hurdles, Yardsticks, Goals, Objectives, Benchmarks, and Triggers.....	275
9.5	Summary.....	277
10	Downsides of Metrics	279
10.1	Numbers Don't Always Tell the Whole Story	279
10.2	Scoring Political Points through Metrics	281
10.3	Implausible Deniability	282
10.4	Metrics Gaps	283
10.5	On Being Good Enough	284
10.6	What <i>Not</i> to Measure	285
10.7	Summary.....	287
11	Using PRAGMATIC Metrics in Practice	289
11.1	Gathering Raw Data.....	290
11.1.1	Sampling	290
11.1.2	Automated Data Sources	291
11.1.3	Observations, Surveys, and Interviews	293
11.1.4	Online or In-Person Surveys.....	294

11.1.5	Scoring Scales	295
11.1.6	Audits, Reviews, and Studies	296
11.2	Data Analysis and Statistics	297
11.3	Data Presentation	302
11.3.1	General Considerations	302
11.3.2	Analytical Tools and Techniques	303
11.3.3	Reporting Tools and Techniques	305
11.3.4	Presentational Tools and Techniques	307
11.3.5	Graphs, Figures, Diagrams, and Illustrations	310
11.3.6	Drawing Attention to Specific Issues	315
11.4	Using, Reacting to, and Responding to Metrics	316
11.4.1	Periodic versus Event-Driven Reporting	318
11.5	Summary.....	319
12	Case Study.....	321
12.1	The Context: Acme Enterprises, Inc.	322
12.2	Information Security Metrics for C-Suite.....	323
12.2.1	Information Security Metrics for the CEO.....	328
12.2.2	Information Security Metrics for the CIO	339
12.2.3	Information Security Metrics for the CISO	342
12.2.4	Information Security Metrics for the CFO	348
12.2.5	Information Security Metrics for the VP of Production....	349
12.2.6	Information Security Metrics for the VP of Marketing ...	352
12.3	Information Security Metrics for Management and Operations.....	358
12.4	Information Security Metrics for External Stakeholders	359
12.5	Acme's Information Security Measurement System	360
12.6	Summary.....	361
13	Conclusions	363
13.1	Take-Home Lessons from This Book	364
13.1.1	On Pragmatism and Being PRAGMATIC	364
13.1.2	On Giving You the Confidence and Skills to Have a Go	365
13.1.3	On Improving the Quality of Your Management Information through Metametrics.....	366
13.1.4	On Improving Metrics of All Sorts.....	367
13.2	Your Chance to Advance the Profession and the Practice of Metrics	367
13.3	An Action Plan to Take Away	369
13.4	Summary.....	370
Appendix A:	PRAGMATIC Criteria	377
Appendix B:	Business Model of Information Security (BMIS).....	381
Appendix C:	Capability Maturity Model (CMM).....	385

x ■ Contents

Level 1—Initial	385
Level 2—Repeatable.....	386
Level 3—Defined.....	386
Level 4—Managed.....	386
Level 5—Optimizing	387
Appendix D: Example Opinion Survey Form	389
Security Awareness Survey on Malware	389
Appendix E: SABSA Security Attributes Table	391
Appendix F: Prototype Metrics Catalog.....	411
Appendix G: Effect of Weighting the PRAGMATIC Criteria	427
Appendix H: ISO27k Maturity Scale Metrics.....	431
Appendix I: Sample Management Survey	475
Appendix J: Observer Bias	477
Appendix K: Observer Calibration	481
Appendix L: Bibliography	483

Foreword

Information assurance (IA) has suffered for decades from the lack of sound quantitative methods for coping with risk and evaluating alternative strategies for allocating resources wisely in the fight against errors and attacks on our information systems.

All of us involved in IA maneuver through competing frameworks for choosing and implementing defenses; unfortunately, all too often we rely on the equivalent of word-of-mouth recommendations—*industry best practices*—in choosing particular paths. As our field matures, we must learn from other professions where methods for evaluating the quality of approaches have shifted from purely intuitive approaches to more systematic and repeatable methods.

The authors of this book have contributed their experience and creativity to present a valuable methodology for creating and evaluating elements of security management. Throughout the work, they emphasize how important it is to use *heuristics* rather than rigid rules in any field that changes constantly.

Security of all kinds suffers from the fundamental difficulty that if security measures work, there's *less* evidence that the measures were necessary, at least for non-professional observers such as non-technical managers. Without sound *metrics*, we are in the position of passersby who encounter a man swinging plucked chickens around his head while he stands on a street corner: asked why he is doing that, he answers, "To keep the flying elephants away." "But there are no flying elephants," respond the befuddled observers. He crows triumphantly, "See? It works!"

Without defining, testing, and refining metrics, our profession will continue to be subject to the legitimate question, "How do you know?" How do we know if our proposals—our proposed spending, our proposed topology, our proposed changes—are reasonable? Why do we choose one set of responses over another? And how will we measure the results of our methods to evaluate their effectiveness and their efficiency?

In addition to supporting the development of IA, the methods presented in this text will reach professionals in fields that will benefit from good, *PRAGMATIC* metrics.

xii ■ Foreword

Thanks to W. Krag Broby and Gary Hinson, I expect to see dramatic changes in our ability to analyze our security options, explain our choices, and measure our results.

M. E. Kabay, PhD, CISSP-ISSMP

Professor of Computer Information Systems

School of Business Management

Norwich University, Northfield, Vermont

Preface

Does your organization have a meaningful, worthwhile suite of information security measurements in place? No? Well then how exactly *are* you managing your information security risks and controls? Let's guess: a pinch of good practices, a sprinkling of international standards, and a large measure of gut feel?!

Whereas most previous publications in this field have been either academic or narrow in scope, we have developed an eminently practical and rational approach to selecting information metrics that work. At its heart, the PRAGMATIC method is simply a tool to identify which of the thousands of possible security metrics are actually worth adopting. That claim may seem trivial if you have not personally struggled with this very issue, but trust us, it's a Big Deal. Sifting the wheat from the chaff is never easy, but at least now we have a way to differentiate grains from husks. Hitherto, they all looked much the same—a uniformly bland shade of brown. PRAGMATIC security metrics appear in full glorious Technicolor™, and not merely 2D or 3D but 9D!

Writing this book was a surprisingly enjoyable labor. We came together serendipitously at a Wellington hotel in New Zealand where both of us just happened to be working on security metrics—Krag delivering a two-day metrics course, Gary co-leading a one-day metrics workshop for the local ISACA chapter. We instantly realized we had a lot in common, not least a sense of humor and a love of fine red wine that made our first encounter a memorable experience. Our shared passion for information security metrics and the belief that *there has to be a better way* drove us together in the search for enlightenment.

Our decision to co-author this book was momentous, not least for the fact that although Krag had already written books on information security governance and metrics, the only book Gary had written was his PhD thesis—many moons ago, and on microbial genetics at that!

At the time we agreed to collaborate, we had not invented PRAGMATIC. The PRAGMATIC concept mysteriously emerged from our early discussions, initially as a way to align our thoughts, but it soon became evident that we had chanced upon something uniquely valuable. The process of evaluating, comparing between, considering, and eventually choosing security metrics solved a vexatious problem

xiv ■ Preface

affecting practically everyone who gets into security metrics. Simply stated, we stumbled on the way to answer the deceptively simple/naïve question, “What should we measure?,” and that answer, in turn, opened up entirely new horizons. Many previously intractable information security management problems become solvable through PRAGMATIC metrics, or rather through the availability of meaningful, factual data on which to base important decisions.

Aside from information security, we are intrigued at the prospect of using the PRAGMATIC approach to develop and select worthwhile metrics in different fields of management—not just closely allied areas such as governance, risk management, and compliance but almost anything in fact. If you are an expert in sports management, financial management, HR management, engineering management, strategic management, or some other specialty who is inspired by this book to develop PRAGMATIC metrics in your context, please do get in touch with the authors through www.SecurityMetametrics.com. We’d love to work with you on this.

Acknowledgments

This book was inspired by other experts in the field, many of whom are cited in the text. If you are truly serious about information security metrics, do check out the references for the fascinating wealth of knowledge they contain. We are genuinely grateful to all those who came before us and look forward to seeing the PRAGMATIC approach being widely adopted and adapted.

On a basic note, Google's free cloud-based collaborative working facilities made actually writing the book much easier than more traditional approaches, especially given the thousands of miles and several time zones separating us. We drafted the book using Google Drive, and established a Google Groups forum to continue the discussion with you (visit www.SecurityMetametrics.com for details).

We thank Rob Slade and Dan Swanson for their insightful feedback on early drafts. Despite Krag and Gary constantly feeding off each other's inspiration, your gentle feedback and improvement suggestions encouraged us to look beyond the confines of our little world.

Last but not least, we would particularly like to thank our other halves, Melody and Deborah, whose constant love and support means the world to us. Ladies, this book is for you too—the royalties at least.

Free ebooks ==> www.ebook777.com

Office Memorandum



Acme Enterprises, Inc.

From: Chief executive officer
To: Information security manager

Dear John,

I realize we have spoken about this a while ago but I am under renewed pressure from the board to clarify a few things about your budget proposals for the financial year ahead. I need your assistance urgently as I am busy preparing for our annual strategy off site. Please, would you address the following issues in writing before the next board meeting at the end of this month as succinctly as you can:

- a. We have spent a small fortune on information security in the past three years: naturally, this seemed justified at the time, but is it perfectly reasonable for the board to ask what we have actually achieved in the way of a return on our investment to date? Can you put a figure on it? Can you demonstrate the value?
- b. How does our information security stack up against our peers in the industry? How secure are we, and how secure do we need to be? Some of the more cynical members of the board are starting to express the opinion that we are

xviii ■ Office Memorandum

going for gold when silver will do, and I must admit I have some sympathy for that viewpoint. However, if you give me the ammunition for a robust response, that will help immensely in terms of deflecting some of the pressure to other cost centers.

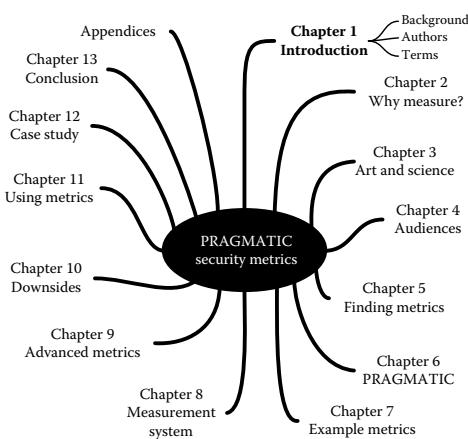
- c. If budget cuts are necessary (which looks increasingly likely), in which areas can we safely trim back on security spending without jeopardizing the excellent progress we have already made? I appreciate that you are reluctant even to entertain the possibility, but I'm sure you will agree that it is better for us to be prepared for this eventuality and deal with it rationally now than to have it imposed upon us later in the process. I should point out that information security is not being singled out for this. We all share the pain of these economically challenging times.

Looking forward maybe three to five years, can you give us a clearer picture of how the information security management system will pan out? The board and the executive managers are understandably concerned about their personal liabilities if we should fail in our compliance and governance obligations.

Regards,
Fred B.
CEO

Chapter 1

Introduction



When a group of business executives was asked what value they found in the security reports they received, the consistent answer was “not much.”

Mathew Schwartz

This quotation from Mathew Schwartz rings a big bell for us. On a good day, we suspect we are gradually becoming submerged in a vast sea of data, struggling to find any useful pieces of information to cling to. On a bad day, we know we’re already too late, and the weak signals we’re hunting for are lost forever in the noise. We have to deal not only with memos and reports from our esteemed colleagues, but with an endless stream of emails, phone calls, blogs, Tweets, and more. In the security arena, it seems as if there’s another security survey published every week,

2 ■ PRAGMATIC Security Metrics

not to mention a gazillion white papers, vital briefings, and urgent advisories.* And to cap it all, Google finds us far more than we could ever hope to read on any topic we care to mention, no matter how obscure, in milliseconds. Contrary to popular opinion, we are not thriving in the midst of an information revolution but drowning under a data tsunami.

1.1 Why Have We Written This Book?

No profession has ever achieved status and creditability prior to developing effective metrics showing cause and effect, providing reliable prognostication, and delivering the information needed by various parts of the organization to make informed decisions. Information security is no different. While practitioners frequently lament the profession's lack of standing with business executives, we continue to fail to provide credible answers to essential questions and reliable evidence for the value of our craft. Most of us only provide management with obscure technical measures that do little to provide needed answers, actionable information, or comfort, let alone assurance.

The reality is that we supply mostly technical metrics to management because they are easy and cheap to collect and perhaps a few others by edict. More than one honest security guy has also confessed to generating[†] metrics purely to support budget requests or to give the *appearance* of being in control. Very few organizations genuinely attempt to manage their information security by the numbers except perhaps in specific and rather limited situations. Gut feeling, conjecture, and guess-work rule the field, representing a rather risky, perhaps even cavalier, approach to the management of information security risks. Is it any wonder, then, that serious information security and privacy incidents are all over the news? That otherwise sound businesses go to the wall when hit by “unanticipated” disasters? That unfortunate patients are overdosed and injured by software-controlled x-ray machines that were meant to cure their ills?

This state is not entirely of our own making, nor are we alone in this: practitioners in other fields, such as risk management, compliance, governance, and many more, also struggle to answer straightforward questions from stakeholders. We may

* We are very conscious that we are adding to your burden by publishing this book. We appreciate that we must compete with all those other demands on your valuable time. We know you are busy and, to be frank, so are we—so much so that it has been tough to clear the space in our diaries to write these words. What kept us going was our overwhelming passion for information security metrics and the thought that maybe, just maybe, we have *something important to say*. See what you think.

[†] Note: We said “generating,” not “measuring”! Security metrics should surely *reduce*, not *increase*, the level of FUD (fear, uncertainty, and doubt)—a point raised by Jaquith (2007) and covered further in Chapter 10.

not have broken security metrics, but it is a reasonable assumption that we will be the ones tasked with fixing the problem!

Few would argue with the need for better information security metrics, enabling organizations to provide measures as the basis for sound information security decisions and improve their risk management and controls in a more systematic, informed way. Without decent metrics,

- Information security professionals are, in practice, managing security largely on the basis of experience, gut feeling, accepted wisdom, faith, standards, and—let's be honest here—a good dose of sheer finger-in-the-air guesswork. “Do this because...er...because it’s the right thing to do” or because *someone* has tagged it a “best practice.” After all, so-called best practices are just a poor substitute for real knowledge and experience. The uninformed just-do-it approach is even evident in many information security and privacy laws and regulations, plus most corporate security policies.
- Management is even more divorced from reality, depending heavily on its faith in information security professionals to keep the organization’s information assets (plus those in its care, control, or custody belonging to customers, partners, suppliers, employees, and, in some cases, the general public) sufficiently free of risk without truly understanding what “sufficiently free of risk” actually means in this context.
- The status (quality, coverage, efficiency, etc.) of the organization’s information security controls is uncertain, the residual level of information security risks even more so.
- Budgeting for and investing in information security is a matter of making lots of assumptions and projections and basically comes down to ill-informed judgment, meaning we don’t know if we are spending enough or too much on security, nor whether we could spend more wisely and appropriately.
- Improving information security is at least as much a matter of good luck as good judgment with the distinct possibility that some of the changes we make are actually retrograde steps, and we may well be totally missing out on significant improvement opportunities that we simply don’t appreciate at all or substantially undervalue.

1.2 What’s Different about This Metrics Book?

Perhaps as a consequence of the way the field of information security has developed from IT security,* current practice in security metrics seems to be driven by the availability of raw data from firewalls, spam filters, and antivirus systems. When it comes to measuring security, many organizations completely ignore the host of

* We offer a condensed history of security metrics in Chapter 8.

4 ■ PRAGMATIC Security Metrics

nontechnical factors that are equally important to managing information security in a way that truly supports the organization's business objectives.

Time and again, we read articles and blogs proposing shopping lists of possible security metrics with the implication being that readers ought to consider and select from the lists, yet how they might actually do so, and the basis on which they are considering and selecting, is seldom even mentioned, let alone explained.

Many of the existing security metrics books and standards are rather academic or theoretical in style, making it hard for busy practitioners to understand, much less apply, them in the workplace. What's worse, some of the suggested metrics approaches are so complex that it would take a cadre of quants or statisticians to derive anything useful, and a few miss the mark completely. There is little obvious consensus on the general nature, approach, or specifics of security metrics. We are not blaming the authors as such: this is characteristic of an immature field of study, one still actively developing.

We believe we can do better, and the hope is that, with our help, so can you. We don't have *all* the answers, unfortunately, but we believe we know how to get some of them, and we know enough about the topic to provide worthwhile advice that is usable immediately. In particular, you will shortly find out how to select and use more worthwhile information security metrics, metrics that will actually mean something and will help you in your job.

This book is our effort to develop a *practical* approach to developing, testing, and operating a set of metrics that effectively support a business, providing management with the information needed to make crucial decisions on risk, security, control, assurance, and governance. Many organizations have endeavored toward this end, including International Organization for Standardization/International Electrotechnical Committee (ISO/IEC), National Institute of Standards and Technology, Carnegie Mellon University, and numerous others, but all have struggled to provide advice that is both solidly based and helpful to information security professionals in the enormous variety of organizations that take information security seriously. Our approach is different, one we believe will substantially advance the field while, at the same time, complementing and extending other methods. That's a bold claim to be sure, but at the very least, we sincerely hope to infect you with a little of our passion for information security metrics.

You could say this is a cookbook of ingredients, recipes, and techniques allowing information security practitioners to cook up their own unique set of information security metrics. In short, our objective is to provide you the tools to be a more effective information security manager.*

* We normally use the term "information security manager" throughout the book, meaning the most senior professional dedicated to the management of information security. In some organizations, this would be the chief information security officer (CISO), chief security officer (CSO), senior agency information security officer (SAISO), security director, security manager, information security officer, information security analyst, or someone else. You might not even have someone dedicated full time to information security, specifically, but we hope *someone* is responsible for information security. Please forgive us if we stick to "information security manager" for brevity. We leave it to you to substitute the term that is appropriate in your organization.

1.3 Who Are We Writing This For?

The primary audience we have in mind for this book is *information security professionals*, particularly the more qualified and experienced practitioners and managers who *need* to measure various strategic, tactical/managerial, and operational aspects of information security in order to manage and improve them.* Metrics are the dials and indicators you need to make *systematic* improvements to security machinery, enhance credibility with management, and, ultimately, improve the functioning and sustainability of your organization. We are also writing for the *directors* and *managers* accountable for information security, risk management, compliance, assurance, and governance. Naturally, you want to measure various strategic aspects of information security in order to direct them for best effect as well as ensuring alignment with business objectives. We'd like to give you the ammunition both to convince your fellow managers that information security deserves their support, but also to challenge information security and risk management investment proposals that may come before you—not necessarily because we think they are bad, but rather because rational and robust challenge leads to better proposals and more informed decisions.

We truly believe the tools and methods described in this book have value and application well beyond the narrow field of information security. Therefore, we are writing for other *metrics and measurement nuts*. We look forward to the creative ways you find to adapt the PRAGMATIC approach and build measurement systems for your diverse areas of specialty.

Finally, we hope the book has value for information security and risk management *students* at undergraduate and postgraduate levels. A sound understanding of information security metrics may be the very edge you need to land your next job. We also hint at the many ways in which you can help us progress the field through further research.

1.4 Who Are We?

And what gives us the bare-faced cheek to spout on about this stuff as if we have a clue?

1.4.1 W. Krag Brotby

W. Krag Brotby has 30 years of experience in the area of enterprise computer security architecture, governance, risk, and metrics and is a Certified Information

* The distinction between strategy, tactics/management, and routine operations is a recurring theme in this book. Other security metrics authors mostly cover the operational level; some cover management, but few cover strategy.

6 ■ PRAGMATIC Security Metrics

Security Manager (CISM) and Certified in the Governance of Enterprise Information Technology qualifications. Krag is a CISM trainer and has developed a number of related courses in governance, metrics, governance-risk-compliance (GRC), and risk and trained thousands on five continents during the past decade.

Krag's experience includes intensive involvement in current and emerging security architectures, IT and information security metrics, and governance. He holds a foundation patent for digital rights management and has published a variety of technical and IT security-related articles and books. Krag has served as principal author and editor of the *CISM Review Manual* (ISACA 2012) since 2005, and is the researcher and author of the widely circulated *Information Security Governance: Guidance for Boards of Directors and Executive Management* (ITGI 2006), and *Information Security Governance: Guidance for Information Security Managers* (ITGI 2008b) as well as a new approach to *Information Security Management Metrics* (Brotby 2009a) and *Information Security Governance: A Practical Development and Implementation Approach* (Brotby 2009b).

Krag has served on ISACA's Security Practice Development Committee. He was appointed to the Test Enhancement Committee, responsible for testing development, and to the committee developing a systems approach to information security called the Business Model for Information Security (BMIS). He received the 2009 ISACA John W. Lainhart IV Common Body of Knowledge Award for noteworthy contributions to the information security body of knowledge for the benefit of the global information security community.

Krag is a member of the California High Tech Task Force Steering Committee, an advisory board for law enforcement. He is a frequent workshop presenter and speaker at conferences globally and lectures on information security governance; metrics; information security management; and GRC and CISM preparation throughout Oceania, Asia, Europe, the Middle East, and North America. As a practitioner in the security industry for three decades, Krag was the principal Xerox BASIA enterprise security architect and managed the proof-of-concept project, pilot, and global PKI implementation plan. He was a principal architect of the SWIFT Next Gen PKI security architecture; served as technical director at RAND Corporation for the cyber assurance initiative; as chief security strategist, was the PKI architect for TransactPlus, a J.P. Morgan spinoff; and developed policies and standards for a number of organizations, including the Australian Post Office and several U.S. banks.

Recent consulting engagements include security governance projects for the Australia Post, New Zealand Inland Revenue, and Singapore Infocom Development Agency. Clients have included Microsoft, Unisys, AT&T, BP Alyeska, Countrywide Financial, Informix, Visa, VeriSign, Digital Signature Trust, Zantaz, Bank Al-Bilad, J.P. Morgan Chase, KeyBank, Certicom, and Paycom, among others. He has served on the board of advisors for Signet Assurance and has been involved in significant trade secret theft cases in the Silicon Valley.

1.4.2 Gary Hinson

Despite his largely technical background, Dr. Gary Hinson, PhD, MBA, CISSP, has an abiding interest in human factors—the people side as opposed to the purely technical aspects of information security and governance. Gary's professional career stretches back to the mid-1980s as both a practitioner and manager in the fields of IT system and network administration, information security, and IT auditing. He has worked for some well-known multinationals in the pharmaceuticals/life sciences, utilities, IT, engineering, defense, and financial services industries, mostly in the United Kingdom and Europe. He emigrated to New Zealand in 2005 and now lives on a "lifestyle block" surrounded by more sheep than people.

In the course of his work, Gary has developed or picked up and used a variety of information security metrics. Admittedly, they didn't all work out, but such is the nature of this developing field (Hinson 2006). In relation to programs to implement information security management systems, for example, Gary had some success using conventional project management metrics to guide the implementation activities and discuss progress with senior managers. However, management seemed curiously disinterested in measuring the business benefits achieved by their security investments despite Gary having laid out the basis for measurement in the original business cases. And so started his search for *a better way*.

Since 2000, Gary has been consulting in information security, originally for a specialist security consultancy in London and then for IsecT Ltd., his own firm. Gary designed, developed, and, in 2003, launched NoticeBored (www.NoticeBored.com), an innovative information security awareness subscription service. NoticeBored has kept him busy ever since, researching and writing awareness materials for subscribers covering a different information security topic each month. One of the regular monthly awareness deliverables from NoticeBored is a management-level awareness briefing proposing and discussing potential metrics associated with each month's information security topic*—for example, a suite of metrics concerning the management of incidents was delivered with a host of other awareness materials about incident management.

Gary has been a passionate fan of the ISO/IEC 27000-series "ISO27k" information security management standards since shortly *before* BS 7799 was first released nearly two decades ago. He contributes to the continued development of ISO27k through New Zealand's membership of SC27, the ISO/IEC committee responsible for them, although he arrived in NZ too late to influence ISO/IEC 27004:2009 on information security measurements, unfortunately (we have more to say on '27004 below!). To find out what ISO27k can do for your organization,

* At the time this book is being written, we are not aware of any other security awareness service offering security metrics as such, but it will be interesting to see whether any of IsecT's competitors read this book, take the hint, and follow suit. We'd be flattered in fact!

8 ■ PRAGMATIC Security Metrics

visit www.ISO27001security.com to explore the standards, find out about new developments, and join ISO27k Forum, the email reflector for a global user group.

Before all that, Gary was a scientist researching bacterial genetics at the universities of York and Leicester in the United Kingdom. He has long since lost touch with the cut and thrust of gene cloning, DNA fingerprinting, and all that, but despite recently discovering his creative streak through NoticeBored, the rational scientist and metrician still lurks deep within him. So seven years of university study was not a total waste after all.

1.5 What We'll Be Talking about

It is a reasonable conjecture that many information security compromises, breaches, and other incidents represent failed, inadequate, or missing controls, which, in turn, flow from failures of security management and, quite often, a commensurate lack of suitable metrics. Metrics give management the information needed to identify situations where other* information security controls do not adequately mitigate unacceptable information security risks and to quantify the extent of the mismatch. Quantification allows management to make appropriate, proportionate responses; to allocate finite resources according to sensible priorities; and, in fact, to determine whether the resources are adequate.

Quantification of information security is all very well in theory but, evidently, not so straightforward in practice. While security metrics have long been considered something *nice* to have, few organizations actually make the effort needed to identify, measure, and report parameters that are important for management to manage information security. Presumably, security metrics are deemed either *too hard* or *too costly* (which mostly means too difficult). It is also apparent that some executives don't want too much information; presumably, so they can feign ignorance in the face of eventual disaster.

This book describes, in detail, how to go about designing a system for measuring information security that gives management the essential information they need. Rather than simply discussing a whole bunch of security metrics and leaving it up to you, the reader, to determine which ones (if any!) are worth using, we explain a structured method for identifying potential metrics, assessing them rationally, ranking them, and selecting the few that have the most value. In the course of this book, we will help you figure out who your security metrics are intended for (i.e., the metrics audiences), what information they need (metrics specifications), and how to integrate individual metrics into a comprehensive system or suite such that they support each other.

* Metrics are themselves a form of control—management as opposed to information security control, that is.

Tip: In Chapter 6, we explain the notion of PRAGMATIC scores that we will be returning to and using throughout the book. More than just a catchy acronym, the PRAGMATIC approach we are describing is designed to be pragmatic in the ordinary everyday meaning of the word. Look out for the metrics tips and examples dotted throughout the book, too.

Now, before we get too carried away with the idea of metrics, it's worth reminding ourselves that we are dealing with probabilities here, not certainties. Even a "perfect" suite of information security metrics would not magically give us the ability to predict or control the future under all circumstances. It will put us in a better position than if we had no metrics at all or, perhaps, a half-baked security measurement system with various gaps and unfounded assumptions and will allow management to plan and implement security more rationally and sensibly, but we cannot guarantee complete security. Just as the near-perfect metrics of an airliner cannot guarantee good weather and a smooth flight, neither can good information security metrics provide assurance that there will never be incidents or that decisions will always be optimal. On the other hand, just as flying a jetliner without those extensive metrics virtually guarantees eventual disaster, so attempting to navigate an information security program without adequate metrics also creates a high probability of adverse consequences.

1.6 Defining Our Terminology

The dictionary definitions of terms such as "metric" and "metrician" are not quite right for our purposes because we are not concerned here with the meter, rhythm, or tempo of a verse, nor the decimal metric system. We implicitly know what we mean by "metrics," and the people we deal with (not just information security professionals) don't appear to have any trouble with the term, but once we start to use distinct words such as "measure" and "measurement" with different meanings, things soon get hazy; hence, we probably ought to clarify the terminology *as we are using it* to avoid confusion:^{*}

- Governance: the act of governing through mandating a set of rules and regulations regarding the actions of individuals within the organization, plus the directive, control, and feedback processes to ensure their compliance.

* We are being pragmatic. These are our unofficial working definitions, not precise, concise, etymologically correct dictionary definitions, but they suit our purposes for the book. The language is evolving along with the field of study.

10 ■ PRAGMATIC Security Metrics

- Indicator: something that gives an indication, that is, an indirect, vague, and/or imprecise measure that may not be strongly correlated with the subject of measurement.
- Instrument: short for “measuring instrument,” that is, a device for measuring.
- Measure: (verb) to determine one or more parameters of something; (noun) short for measurement, for example, the meter (“metre” outside the United States) is a length measure.*
- Measurement: the value of a parameter for something, ideally expressed in defined units with an appropriate degree of precision, for example, “the height measurement of the door is 1.98 meters.”
- Metametric: information about metrics (explained further in Section 6.1).
- Metric: a measurement in relation to one or more points of reference.
- Metrication: the process of selecting and applying metrics to improve the management of something.
- Metrician: a metrics practitioner—someone fascinated with metrics who develops and uses metrics.

1.7 What We Expect of You, the Reader

While we are writing for a range of readers with differing experience and expertise, we accept that metrics is an advanced, cutting-edge topic in the field of information security. It demands deep thought. Unfortunately, much as we would love to do so, we cannot simply provide you with a short list of security things to measure. Your specific needs are unique, and what’s more, they will change over time as your measurement system matures and the organization learns and adapts (at least partly in response to previous metrics!). It has often been said that what gets measured, gets done, so the very presence of new metrics is likely to change the security focus of the recipients of those metrics. It’s all very dynamic and difficult, we know, but as we said, the reason we have published this book is that we have *something to say*—not just more noise, but actual signal.

Please don’t just skim quickly through and put this book aside to collect dust on your bookshelf forevermore: if you don’t have the time to read it cover to cover right now (and who does?), dip in, think about what we’re saying, and start to try things out for yourself. Right now, many of the things that you feel are important in information security management may seem all but impossible to measure, so park them for a while, continue reading and learning about security metrics, and come back to them later with some more creative approaches. Meanwhile, work on the easier stuff.

* In information security, “measure” is commonly used as a short form of “countermeasure,” meaning a control. We try to avoid using it in that sense here.

Chapter 6 is the crux of the book where we elaborate on the PRAGMATIC method, an eminently practical and straightforward tool to help you choose rationally between the *thousands* of potential security metrics on offer. Chapter 7 uses the PRAGMATIC method to score and explore more than 150 security metrics examples. If you're puzzled about how to make this approach actually work in your organization, Chapter 12 offers a case study/worked example demonstrating the entire process in the context of a hypothetical company choosing security metrics for key audiences.

The book is peppered with more than 150 pragmatic *tips*, including shortcuts and practical suggestions to make your life a bit easier, such as the innovative ISO27k-aligned maturity scoring scales in Appendix H. Please read the footnotes* and check out the references if we haven't quite satisfied your incessant thirst for knowledge.

By all means scribble notes in the margins (provided you actually own the book, anyway!), and share your metrics experiences, queries, and answers with other readers through the security metrics disorder (SMD) Forum[†] at www.SecurityMetametrics.com.

Pick the suggestions that look the most attractive, relevant, and useful to you, and give them a go. Make use of the security data you have in hand, and start teasing out those valuable nuggets of information that lurk deep within.

Then come back for more. These words will still be here, waiting patiently to inspire you the next time you grab this book from your bookshelf and blow away the dust.

1.8 Summary

Chapter 1 set the scene for the book, describing who we are and who we think you are and explaining why we have provided quite so many tips and footnotes. We defined our terminology and explained that we hope the reader will play an active part in developing the field.

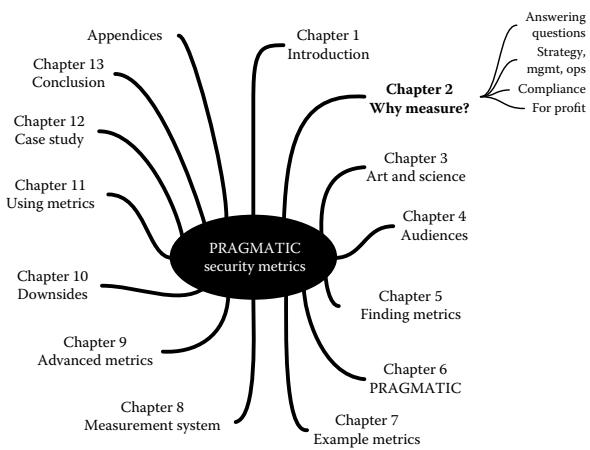
* Thank you. Actually, you might want to ignore the footnotes on first reading. Come back to them later when you have a better picture of the whole thing, and it's time to go beyond merely *reading about* to *doing* security metrics. We've raised quite a few additional/advanced considerations in these footnotes, plus various anecdotes, but we appreciate that they can be distracting. Excuse our quirky tongue-in-cheek asides...oh and *do* try not to get yourself in a lather over whether we should be using "measure" or "measurement" instead of "metric": We know, we know...

[†] Read Section 3.7 first.

Free ebooks ==> www.ebook777.com

Chapter 2

Why Measure Information Security?



Every CSO should have half a dozen dials to watch on a regular basis. These indicators could be “survival metrics,” the hot buttons on a dashboard you are expected to address that monitor the wellness of your organization or an issue of particular concern to management.

George K. Campbell (2006)

Given that so many organizations evidently cope *without* much in the way of information security metrics, it seems reasonable to explore the reasons why we believe measuring information security is worthwhile although not absolutely essential.

14 ■ PRAGMATIC Security Metrics

Good practices may, in fact, suffice in some circumstances, but a one-size-fits-all approach will never be optimal and inevitably will result in overprotection of some assets and under-protection of others.

From our experience, we believe there is a genuine and increasingly urgent need for viable metrics in information security. While, to date, the profession has generally muddled through with almost no rational, sound, and defensible security measurements, the situation is simply not sustainable over the long term. We are fast approaching and, in some cases, already exceeding the limits of the information security manager's gut feeling, qualifications, and experience, coupled with the use of ill-defined and generic good or so-called best practices, as a basis for extremely important security and risk management decisions. While not so common these days, there are still those who contend that as long as you implement best practices, you don't need extensive metrics. However, best practices are an inadequate substitute for genuine knowledge. What may be best in one organization may be too costly and excessive in another or, in some cases, wholly inadequate. Without metrics, how would you ever know?*

Improving information security is becoming ever harder given that we have already, to a fair degree, harvested the low-hanging fruit. And, unfortunately, as our rate of improvement declines, there are clear signs that organized criminals, hackers, saboteurs, industrial spies, fraudsters, malware authors, and terrorists are gaining the upper hand, perceptibly raising the stakes. It is not far off the mark to suggest that the profession is in, or is fast approaching, a crisis of confidence. We're winning occasional battles but losing the war. When experienced security professionals turn from being just ordinarily pessimistic and risk-averse to jaundiced and cynical and retiring or leaving the profession for less stressful occupations, is it any wonder that business managers and stakeholders begin to lose faith in our abilities?

The bulk of this chapter consists of a string of rhetorical questions or issues that raise their ugly heads in some form in most organizations at some point. Count yourself lucky if you haven't been asked them yet: it's just a matter of time.

The points that follow would form the basis on which one might justify the investment needed to specify, design, and use an *information security measurement system*, leading to (we hope) a convincing business case for such a system and, potentially, justifications supporting at least the initial suite of security metrics that populate it. Don't fret: we will discuss the measurement system, the selection of metrics, and all that in later chapters, but let's start by considering the fundamental requirement for security metrics.

* We hear, "You can't manage what you can't measure" quite often. It's an old saw. The phrase has a ring of truth to it, but actually we *do* manage unmeasured things all the time, just not particularly well! We contend that a lot of information security managers have been struggling to manage information security with inadequate measures because they had no alternative—until now.

Tip: This is a deceptively important chapter, more than just a way to introduce the book. Please don't speed-read too quickly in an effort to get to the real meat, or you might just miss the target completely. While you consider the questions we raise here, ask yourself other similar questions that are relevant to you and your organization, your management, your information security situation. Better yet, consider the way in which we have phrased the questions as, in so doing, we are subtly framing the problem space. Posing appropriate questions is the real art to information security metrics. Compared to that, answering them is the easy part! If you gain nothing else from this book, we sincerely hope you learn the value of gently guiding your management into posing better questions of information security. If they are questions you can answer, so much the better! And if you are a manager, pose away!

2.1 To Answer Awkward Management Questions

Your organization is not ready for a metrics program if you do not have a clear, formal understanding of your goals; strategic plans; policies, procedures and guidelines; existing, repeatable processes; and open lines of communication with stakeholders.

Samuel A. Merrell

We opened this book with an imaginary internal memo from the CEO to the information security manager, urgently seeking answers to a bunch of questions that turn out to be rather difficult to answer without the ability to measure various aspects of information security. Let's now explore some more of those awkward questions:

- **Are we secure enough?** Realistic managers should not actually anticipate the organization being perfectly secure and free of all information security incidents, but it is perfectly reasonable for them to seek assurance that avoidable incidents are (mostly) being avoided while any incidents that do occur cause minimal (ideally negligible) or, at least, manageable impacts. Management also wants to be reasonably confident that the information security measures in place are adequate to address the risks. This is a rational—if naive—question for management to pose, yet it is fiendishly difficult to answer without metrics and, to be frank, still tricky to address even with solid metrics. “Are we secure enough?” is arguably the \$6 million question, the elephant in the security metrics room.
- **Are we *more* or *less* secure than our peers?** Assuming that our organization is, in fact, comparable with industry peers, we don't want to overspend or underspend on security, so they could be our benchmark. On the other

hand, *appearing* to be more secure than them may actually be worthwhile, in terms of both the brand value of security and in deterring potential adversaries, encouraging them to divert their attentions to our competitors (and, by the way, the same point applies in reverse: are our peers truly as secure as they appear to be?). The fact is that the *perception* of security can be nearly as important as the *reality*. And if we are in a highly regulated industry subject to punitive sanctions, we clearly don't want to be at the bottom of the heap presenting a prime target for enforcement actions.

- **Which are our strongest and weakest security points?** What are the things we can and should build upon, respectively? Note that there is more to this than just identifying and addressing information security vulnerabilities. Security strengths and capabilities (such as multifactor authentication) can be leveraged to develop new lines of business that would be reckless for our less capable competitors.
- **What are our biggest security threats or concerns?** This is important both in the present context and in the future, for instance, in connection with new business ventures or relationships, product lines, processes, or systems. Depending on the business sector, these threats can differ greatly in terms of potential impact.
- **Are we spending (investing) too much or too little on information security, or do we have it about right?** Are we investing wisely, spending on the things that will benefit the organization the most and support its strategic goals? Would additional investment in certain areas be cost-effective (e.g., enabling business processes or opportunities that would otherwise be too risky), and, if so, which are the preferred security investment options? When times are hard, in which areas of information security would it be safest to make cutbacks, and, conversely, which ones would we be foolish or even reckless to cut? **Security metrics can be used both to demonstrate the value of information security and justify the ongoing investment, two activities that challenge even the most seasoned and battle-scarred information security veterans.**
- **Are our security resources allocated optimally?** Do we implement the security technologies *du jour* simply because others do? Have we truly considered the return on investment for major security investments, such as IDS/IPS? Are we perhaps missing out on opportunities to implement more cost-effective information security controls, such as security awareness and training, or generally accepted standards of good security practice?
- **Have we properly and adequately treated all reasonably foreseeable information security risks?** Are any nasty surprises lurking around the corner? This is a complex question because definitions of "properly and adequately" may be called into question if there are incidents, while "reasonably foreseeable" gives management plenty of wiggle room to deny its accountability for poor management decisions.

- **Can we handle compromises, breaches, and other information security incidents effectively and efficiently?** What about more serious ones, including outright disasters? Are we sufficiently well prepared to cope with unknown difficult situations that may arise, or are we operating on a knife edge where one more serious incidents may tip us over?
- **Are we (sufficiently) compliant?** Are we fully compliant with the obligations that really matter? While we must comply fully with many of our security obligations, on some, we may wish to defer full compliance until a more appropriate time, and for a few, we may make a rational management decision that it will be less costly to accept the consequences of noncompliance than to implement security controls purely for the sake of compliance; in other words, full compliance may not be in the organization's best interests. Will the auditors, regulators, and business partners/customers give us a clean bill of health if they review our information security and related matters, such as risk management, governance, and compliance?
- **Are we *best in class*?** Are we perhaps overdoing it, or are we lagging the field in information security? Which parts of our information security management system are performing relatively weakly, and which are leading the way? Would we be able to defend our position on information security to stakeholders, the stock markets, and the news media if probed or if a serious security incident occurred? Can we genuinely claim to have done everything we could to secure customer data? As a number of court cases involving a bank's responsibility for protecting customers' accounts have demonstrated, this is far from a straightforward issue. Legal decisions have differed significantly with nearly identical cases being decided both for and against the banks. Having credible metrics demonstrating not only that the organization has a decent set of security controls in place, but that management takes information security seriously enough to invest and take an interest in the measures, would, we feel, bolster their case. It will not inspire comfort, confidence, and credibility if the CEO or CIO gets all flustered on the witness stand when asked basic questions, such as "When was the last time this happened?" or "How many times has this kind of incident happened before, exactly?"*

In this context, we are amused to note that fully 43% of the ~10,000 respondents to the Global State of Information Security 2012[†] survey consider they are not merely "strategists" but "front-runners" with respect to their approach toward information security (Figure 2.1).

* There's a sting in the tail here, however. Management has no excuse for failing to act on serious security issues that were clearly evident from the metrics. We'll return to that depressing thought in Chapter 10.

† See PwC (2011).

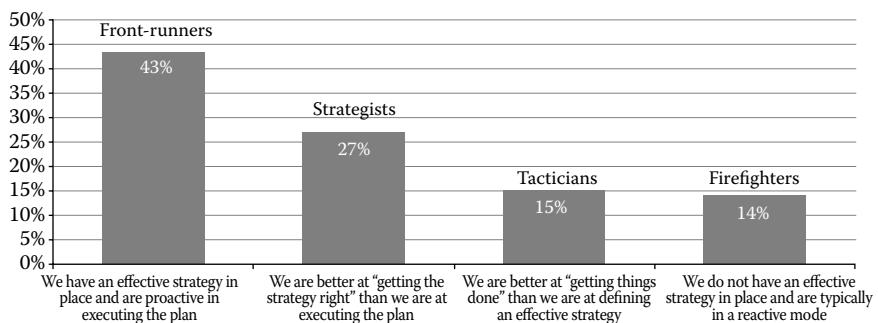


Figure 2.1 Bar chart from security survey. (From PwC. 2012 Global State of Information Security Survey. 14th Annual Survey. www.pwc.com/gx/en/information-security-survey, 2011. With permission.)

And we can't help but wonder if they are all using information security metrics to the best effect.

2.2 To Improve Information Security, Systematically

Our information security controls are never going to be perfect; we know that. Worse still, they seldom remain good enough for long in practice because, despite our efforts, the risks are constantly changing around us, and controls inevitably degrade over time. And it seems that as quickly as we plug the holes in the dam, others appear. We therefore need to update and adapt the security controls to catch up with current risks, at the very least, if not to get ahead of the game where opportunities present themselves. Security improvement is vital because nobody would seriously accept further declining standards, and even stasis is patently not good enough, given the enormous costs of major security incidents that hit the news media every few months.*

It could be argued that we have gotten where we are today mostly through a process of trial and error, hit or miss. Most of us try to learn from our own mistakes, and the best of us also learn from the mistakes made by others. Learning the lessons and making changes to prevent recurrence is perhaps *the* most important part of incident management, yet it's hard to do this if the corporate culture is generally to sweep things under the carpet wherever possible in order to save face and avoid further embarrassment. If we don't even track and record incidents properly and can barely guess at which incidents are costing us the most each month or year, how can we determine which changes are truly worth making? With a system in place to capture the numbers and adopt the learning points from security incidents,

* You could say we are running to stay still.

we can at least recover some of the lost value and move ahead instead of merely keeping pace or falling behind. Capturing, analyzing, and using statistics and other information concerning security incidents is just one example of how we can make the process of improving security more *systematic*.

Other systematic improvements include the following:

- Driving *strategic alignment* between the business and information security, which means identifying and dealing rationally with any discrepancies or, even better, avoiding such discrepancies by integrating strategic information security planning activities with other strategic business planning in areas such as governance, risk management, and compliance, of course, plus business development and new product development.
- Improving *risk management*. Uncertainty is the core issue in risks in all forms. We already know we need to deal with commonplace security incidents, and we would be negligent if we failed to do so adequately. However, we still have choices over how best to deal with them (e.g., balancing deterrent, preventive, detective, and corrective controls and minimizing threats, vulnerabilities, or impacts). With less common incidents, we also face additional decisions, such as which ones we need to address and when we need to address them or whether to simply deal with them as they occur. We need to address information security risks in a rational way (dealing with uncertainty through probability and assurance), for instance, by developing suitable policies, standards, procedures, or guidelines showing how we intend to treat the risks in a way that meets both security and business objectives. We need to evaluate the threats, vulnerabilities, and impacts, which means we really need to measure them. In other words, we need threat metrics, vulnerability metrics, and impact metrics. These will encourage management to dig beneath bland risk scores and heat maps to identify opportunities to address the threats, vulnerabilities, and impacts through security controls and other forms of risk treatment.
- Improving *security management*—understanding information security, risk management, and related fields and appreciating the dependencies and interrelationships. Determining whether the changes we are making or have already made are actually improving things, for example, developing cost-benefit analysis of security investments beyond being merely a way to justify the business case but elaborating on the projected benefits to generate a set of metrics that will allow us to milk every last ounce of value from the investment. Making security changes where necessary, knowing that changes are often interrelated (as a crude example, if we transfer skilled security professionals to particular tasks, whatever tasks they leave behind are probably going to suffer—more on resource management below).
- *Systematically improving security controls.* “Systematically” is an important point. Without decent metrics, security management is rather hit or miss.

20 ■ PRAGMATIC Security Metrics

We are forced into making changes based on gut feeling and instinct without really knowing whether those changes are needed, nor whether things are even going in the right direction. We need to be finding and plugging security gaps before they are exploited, ideally doing so in a risk-aligned manner, that is, dealing first with the most severe and pressing risks as a priority. When resources are limited, we should be able to rein in nonessential spending in order to focus on the parts that really matter, implying that we have more than a vague notion of which bits we can afford to let drift for now.

- *Optimizing the value* of information security. This is a key issue for information security professionals because the department's budget depends on persuading management of the need to invest in information security rather than in other areas; it is equally important for management to know that they are, in fact, getting better returns from security investments than from other options.
- Improving *resource management*, for example, prioritizing information security work (such as security testing of new/changed application systems) relative to other business activities (such as nonsecurity testing and implementation of those systems) and allocating resources effectively, for example, investing in the security infrastructure, being a suite of controls that have multiple applications and so forming the foundation of a solid security structure, but, at the same time, ensuring the infrastructure is sufficiently flexible and suitable for current and future needs.
- For *performance measurement*, allowing us to direct resources and improvement efforts toward the weakest areas of security or, rather, to those that have the greatest potential for improvement.
- Raising *security awareness* in a general sense, for example, using data concerning the frequency of malicious packets received from the Internet to illustrate and reinforce awareness and training messages about the importance of network security.
- *Planning* and sequencing security improvements sensibly, for example, designing and implementing enterprise-wide security architectures comprising common interoperable controls used by many systems.
- *Predicting security risks* based on rational analysis of the prior and current information security situation rather than pure guesswork. The closer we approach certainty, the easier it is to convince management to spend on security and the more confident we are that we are allocating finite resources to the most appropriate areas.

2.3 For Strategic, Tactical, and Operational Reasons

We will explore this aspect further in Chapters 4 and 12.

- *Supporting strategic (long-term) security decisions.* What does the CIO or information security manager really need to know to guide and direct the information security management function confidently in the years ahead? Where are we or, rather, where should we be heading and what are our objectives in order to mature our information security management system and support or enable strategic business initiatives? If information security management were a cruise ship, typical strategic issues would be deciding which global markets to pursue, what strategic partnerships to develop, how many other ships there should be in the fleet, and what their respective roles are. What are the ports of call, what regulations must be dealt with, who are the customers, and what are the risks that must be managed? In other words, where is the organization headed, what are the strategic objectives, and how do we get there?
- *Supporting tactical (day-to-day) security management decisions.* What does the information security manager need to know to plan the department's projects during the weeks and months ahead? Are we heading in the right direction to achieve our strategic objectives? Do we have enough fuel (resources) left to get there? What are the most pressing ship-management issues, and what more do we need to do to prevent everything else becoming urgent too? Many, but not all, technology decisions are tactical in nature. Information security risks should be taken into account when considering the adoption of new technologies, for example, but what does that actually mean in practice? A comparative measure of the information security aspects of different technologies would help management make vital decisions, provided it was both credible and available to them, even if, unfortunately, information security is not the ultimate deciding factor! By analogy: where are we headed on the present voyage, what route should we follow, and how are we getting there? Do we have enough fuel?
- *Supporting operational (hour-by-hour) security decisions.* What information are the information security officers, architects, analysts, and administrators most likely to need when deciding which security tasks to tackle next in the hours and days ahead and how to tackle them? Which way and how far should we turn the ship's rudder? How is the engine doing? Is the fuel pump working correctly?

Leading organizations give considerable attention to base lining, benchmarking, and the collection and analysis of IT performance information. They use a variety of data collection and analysis tools and methods that serve to keep them informed but without imposing unnecessary reporting burdens. They also periodically review the appropriateness of their current measures.

GAO (1998)

2.4 For Compliance and Assurance Purposes

- For *compliance* purposes, including legal, regulatory, and contractual obligations, plus certification against information security good practice standards, such as ISO27k and policies mandated by management. Detailed individual information security measures can be used to disclose the extent of compliance or noncompliance to specific information security requirements, and aggregate metrics can point out whether the organization faces problematic noncompliance with certain laws, regulations, contracts, standards, or policies.
- For *due diligence* (finding out what we ought to be doing) and *due care* (actually doing the things we know we ought to do). In most jurisdictions, due care is a legal standard to do those things that a person of similar competence would do in a similar situation. In the information security context, due diligence involves management making the effort to discover whether the organization faces unacceptable information security risks despite the presence of a variety of information security controls. Some organizations have the role of information asset owners,* meaning managers who are held personally accountable by their peers for the protection of certain information systems, processes, and information. In order to fulfill their obligations, information asset owners are expected to ensure that security risks affecting their information assets are assessed and monitored, decide how to treat the risks (i.e., accept them, avoid them, transfer them to others, or mitigate them through controls), and ensure that the risks are duly treated. Information security metrics derived from risk analysis can inform information asset owners about the significance of the risks. Metrics relating to the coverage and effectiveness of the information security controls and other forms of risk treatment are obviously useful for due care: if the metrics reveal that the controls are inadequate or missing, something needs to be done. Ideal PRAGMATIC metrics take that a stage further by indicating more specifically what ought to be done in advance of any incidents.
- For *assurance and reassurance* purposes. Providing *credible* evidence should help convince auditors, reviewers, assessors, and, ultimately, stakeholders that our information security and risk management practices are sound. While we can't ever be 100% secure, wouldn't it be good for information security, risk management, and IT audit professionals to be able to reassure management and other stakeholders that they are secure enough? Having the numbers to

* Information asset owners feature a number of times in this book. We make no bones about it: We feel the concept is an *excellent*, pragmatic means of holding individuals accountable for protecting valuable corporate information assets assigned to them, which, in turn, forces them to take their information security responsibilities seriously for once.

back up those claims adds credibility and confidence to the declarations and, by the way, reduces stress levels in those making them.

- For *accountability* in situations where an authority, customer, business partner, head office, owner, or other stakeholder has a direct interest in the organization's information security controls. It is neither feasible nor sensible, economically and practically speaking, for all the stakeholders to review or audit an organization's information security arrangements individually. To a certain extent, they can rely on security certification and accreditation schemes (such as ISO/IEC 27001:2005 and PCIDSS) and formal management statements regarding the organization's security status, but how much better would *both* approaches be if they were accompanied by meaningful, well-designed, and, most of all, credible information security metrics?

2.5 To Fill the Vacuum Caused by Our Inability to Measure Security

If we had no information security metrics and did not measure information security at all, here are just a few of the problems we would face:

- Management and other stakeholders would probably assume that information security is not important or at least not as important as the things that *are* measured and reported routinely—like finance, for example. They may say business runs on numbers, but what they really mean is that business runs on dollar figures. If we literally can't put a figure on the value of information security, we're on a losing streak already.
- The information security function would only come to management's attention *after* a major security incident in a distinctly negative light. There would be little management appreciation of the role information security plays in avoiding, preventing, and mitigating many other security incidents or in enabling a range of business activities that would otherwise be too dangerous to undertake.
- Investing in information security would be pure guesswork with no idea whether we are investing enough in the right things. There is a good chance we would not be investing in security at all, except perhaps for compliance with certain obligations, and, even then, it would probably be viewed as an expense, not an investment.
- A strong information security function might be able to use FUD (fear, uncertainty, and doubt) to obtain a budget for whatever it felt like doing with no way for management to determine whether those things were appropriate nor whether they were achieved.

24 ■ PRAGMATIC Security Metrics

- The security manager would only be able to determine when risk was unacceptable by his or her termination.
- If anyone asks us whether we are secure, we would be unable to answer truthfully or provide evidence to back up our assertions.
- Information security incidents would come as a complete surprise or shock out of the blue.
- There would be no way to compare the organization's information security arrangements against requirements, standards, or comparable organizations (benchmarking).

It is noteworthy that in a PWC survey (PWC 2011), a quarter—yes, a quarter—of the ~13,000 global security and IT managers surveyed reported that *they didn't even know if they had any security incidents in the past year*. A third reported not knowing what kind of security events they had or the causes. Given this lamentable lack of the most basic knowledge, we have to wonder what their security budgets are based on.

2.6 To Support the Information Security Manager

Having valid metrics enables business managers to make rational, sensible, and, for that matter, defensible decisions about information security. No longer must they rely entirely on advice from information security professionals or generic good practice standards, laws, and regulations. This has two important consequences for the information security manager:

1. Decisions about whether certain information security risks are acceptable or need to be treated in some way should, by rights, be made by the owners or custodians of the information assets that would be harmed, devalued, or destroyed if the risks materialized, causing security incidents. The information security manager has heretofore been forced to make such decisions on behalf of the information asset owners, either by laying down the rules or by strongly advising management to take a certain course of action. With suitable metrics concerning risks and controls, information asset owners can decide things for themselves. This aligns directly with the governance practice of holding information asset owners personally accountable for protecting and exploiting their information assets.
2. The information security manager can relax a bit. Yes, that is important! Managing information security is a stressful, thankless task without the added pressure of being responsible for security without, in many cases, having the resources to make things adequately secure.

2.7 For Profit!

The ultimate aim of information security is, in a word, sustainability and is achieved through the following:

- *Cutting losses*: minimize information security incidents in number or severity/impact in a cost-effective manner.
- *Increasing assurance*: give management and other stakeholders a degree of confidence that information security risks are in hand and there are no unacceptable risks that exceed the organization's risk appetite.
- *Supporting the business*: enable the organization to conduct business activities that would otherwise be too risky.
- *Enabling rational decisions*: for example, choosing between alternative or complementary forms of risk management (such as incident prevention, incident response, resilience, recovery, and insurance), ideally adopting the most cost-effective approach, or when to take action of some sort, such as adding countermeasures, changing course, or increasing capabilities.

Information security metrics allow us to implement better, more cost-effective security controls that align with and support the organization's business objectives. Furthermore, designing, developing, maturing, and using the *information security measurement system* present opportunities for management to review and reconsider how security impacts those objectives—to some extent, it's chicken and egg: effective security metrics are derived from sound security objectives effectively supporting the business and *vice versa*.

Metrics offer a rational basis on which to challenge the accepted wisdom in information security, for example, using measurements and analysis to prove that certain traditional controls (such as regular password changes) are not only wasteful but may be counterproductive, even harming security. That exemplifies a situation in which metrics may enable us to remove, modify, or moderate security controls: security is not necessarily a matter of continually increasing controls!

Tip: Imagine being in a position to suggest to management that certain security controls might safely be retired and the security budget reduced and having the data to substantiate your claim. Once management overcomes the shock, it's likely your credibility would gain a few notches. Metrics could do that for you. They can also help you and your management allocate what resources you can obtain to best effect.

2.8 For Various Other Reasons

You, your management, or other stakeholders may well have excellent reasons for wanting to measure your information security beyond those we have mentioned so far. Take the U.S. government as an example: it spends a fortune in taxpayers' money through numerous government agencies and is bound to be held accountable in various ways if those agencies fail to perform, for example, if they experience serious information security or privacy incidents. If the incidents were clearly avoidable, questions will surely be asked. U.S. taxpayers and the government are perfectly justified in seeking assurance that the agencies are, in fact, paying sufficient attention to their security and privacy requirements and spending their budgets wisely. The situation is probably much the same for other governments and, in fact, other federal or group structures where security budgets are centrally allocated and monitored or, more importantly, where the ultimate accountability for information security failures ends up...but naturally the details vary between organizations.

In the United States, the Dodd-Frank Wall Street Reform and Consumer Protection Act resulting from the financial meltdown in 2008–2009 is likely to create the requirement for a plethora of new metrics within the financial services industry. The act initially applies to financial organizations, but it is reasonable to assume these provisions will find their way into other sectors that pose risks to the well-being of the economy as a whole. One of the provisions that are of interest to information security is the requirement to form a risk committee that must include a risk management expert. As a consequence, it will become increasingly difficult for management to ignore its responsibility for adequate protection of the organization's assets, including information. In the coming years, we can expect to see interest in risk-related metrics becoming a greater priority and a reduction in the plausible deniability approach that has been common in times past—the “Goodness, I didn't know we had those risks!” or “We don't think cigarettes are addictive and cause lung cancer” executive defense. This statutory provision is summarized thus: “Financial services industry risk committees. This provision of the Dodd-Frank Act calls for certain nonbank, public financial companies and certain public bank holding companies to form a separate risk committee. Based on the legislation, risk committees will be held responsible for risk oversight in the organization. They must include the appropriate number of independent directors, as determined by the board of governors, based on factors that include the nature and size of the organization. They also are required to include at least one risk management expert, as defined by the act” (Deloitte 2010).

Fifty-eight percent of executives polled said [their organizations] have lost sensitive personal information, and for nearly 60 percent of those who have had a breach, it was not an isolated event.

Accenture (2009)

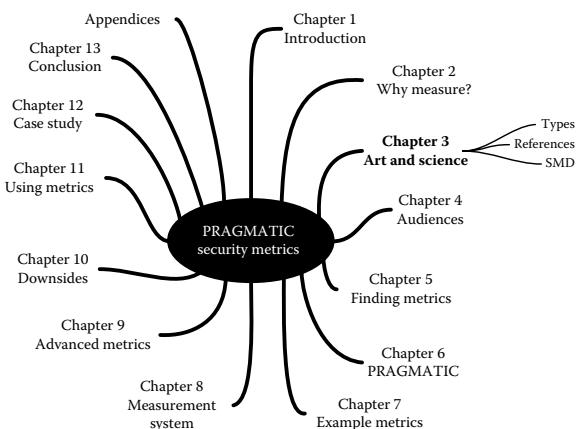
2.9 Summary

This chapter laid out a number of reasons explaining why information security metrics are so important for management, compliance, and so much more. Frankly, we struggle to understand how so many organizations claim to be front-runners in information security pursuant to the PWC Global State of Information Security 2012 study, yet decent security metrics are such a rare exception. It is difficult to understand what basis (any metrics, in fact) they have for believing themselves to be front-runners, other than wishful thinking.

Free ebooks ==> www.ebook777.com

Chapter 3

The Art and Science of Security Metrics



IT metrics are like art. No one can seem to agree on what constitutes a good metric, but everyone seems to know one when they see it.

Ann All

Security metrics is an evolving field of study, involving a combination of purely scientific and not-so-purely scientific approaches as the academics and practitioners feed off each other. While we appreciate the value of the scientific and mathematical principles, theories, and models that underpin metrics and measurements, our particular contribution in writing this book lies far more on the practical side of the fence. We study metrics not for the sake of science, but because they can help

us resolve real-world situations that we face in information security management. Call it applied science if you will, state of the art, perhaps.

In recent years, a number of organizations and individuals have expressed their views and made suggestions on how information security can or should be measured. In this chapter, we consider their advice, comparing and contrasting their approaches with the approach that we favor. If you are serious about security metrics, we encourage you to check out the cited references for yourself (if you haven't already) and draw your own conclusions. Although we are highlighting certain key sources specifically in this chapter, we encourage you to look at the bibliography toward the end of the book for further reading. You may not have the interest to delve too deeply into the field right now, but perhaps after finishing this book and starting to apply the techniques we suggest, you will feel the need for additional background and loftier expositions on security metrics.

3.1 Metrology, the Science of Measurement

Metrology, derived from the Greek word *metron*, is the science of measuring and quantifying things. "Metricians" are the practitioners of metrology. In this book, we are primarily concerned with one relatively narrow and specific form of applied metrology: the practical application of theoretical measurement science in the real world of information security. We also have an interest in the application of metrics to the much broader fields of business management, governance, and risk management, although mostly in the areas where they intersect with information security.

We don't intend to go into detail, but, briefly, here are a few of the important factors in metrology:

- *Precision* concerns the limit of details that can be measured and distinguished.
- *Accuracy* includes aspects such as repeatability.
- *Integrity* is a concern for the measurement data and the systems and processes of measurement.
- *Utility* is about measuring things that matter.

You will find distinct echoes of these considerations and more in the PRAGMATIC method.

3.2 Governance and Management Metrics

Metrics are primarily a *decision support tool for management*. Good metrics provide useful, relevant information to help people—mostly, but not exclusively, managers—make decisions based on a combination of historical events (the context),

what's going on right now (including available resources and constraints), and what is anticipated to occur in the future (the change imperative).

Management metrics and measurement practices in general are continually evolving; for instance, the Balanced Scorecard (Kaplan and Norton 1996) was considered state of the art when it was released well over a decade ago and still remains influential today. It has been adopted and adapted by many organizations and today finds application in a wider variety of ways and situations than its original authors probably conceived.* In contrast, executive information systems that became prevalent a few years back when everything was going online have proven counterproductive in some organizations by focusing management attention on the pretty graphics while, in some cases, hiding or distracting them from important details.

The executive dashboard concept remains intriguing and pops out of the wood-work again every few years. The latest incarnation we've noticed is security information and event management (SIEM). Most dashboards are promoted to the market as metrics systems by pushy software vendors who have found it easy to catch the eye of budget holders with their bright colors and fancy graphics. Most of them report metrics from automated security tools, such as firewalls, antivirus, and intrusion detection/prevention systems because certain technical statistics are readily obtained, but as to whether they are of any practical value for executive managers seems doubtful, in particular, because management needs information beyond the purely technical.

Information security managers find it difficult to justify security initiatives and investments objectively to upper management. This is, in large part, because they can't provide metrics to support their cases because they don't incorporate feedback processes indicating the extent of protection and the effectiveness of security controls implemented previously. This is a systematic issue. Coupled with the inability to quantify information security risks and the effectiveness of proposed controls persuasively, it generally results in a lack of adequate or misdirected investment in security and hence significant underprotection of information resources.

Anything that causes an observable change can be measured by observing the change. The main issue in relation to security metrics is to determine the sort and nature of measurements that provide useful and meaningful information upon which to effectively base decisions—decisions about whether greater control is needed, whether controls are failing and need remediation, or whether existing controls are sufficient or, in fact, excessive.

* In the same way, we hope the PRAGMATIC approach and the concept of metametrics will be widely adopted. We don't consider ourselves the sole guardians or bastions of Truth. We encourage you to consider and build on the ideas we are presenting, finding creative ways to use them that make sense in your specific context. We would *love* you to share your experiences and developments with others. Most of all, we want to give our fellow practitioners a handy tool to make your lives a little easier albeit one of many in your toolboxes.

Metrics can also be used to influence and possibly bring change to a culture. For example, developing good and useful metrics around security and then publishing the results, say, monthly to management may yield a number of beneficial results. For one thing, it will raise the profile of information security. For another, it will make it abundantly clear which way things are headed and can generate a great deal of pressure for improvement. It might serve to expose the security laggards and to reinforce those activities that yield good results.

The point is that information security metrics should serve to inform, facilitate, and guide proper and appropriate decisions to achieve security objectives. That translates into measuring *the right things* and reporting them to *the right people* in *the right format at the right time*:

- The *right things* are those that mean something to the recipients, causing them to make appropriate decisions.
- The *right people* are those that make or at least influence the decisions (see Chapter 4).
- The *right format* is one that effectively communicates—it gets the message across and motivates the recipients to act accordingly (see Chapter 11 for more on data analysis and presentation).
- The *right time* is, of course, before the final decision is made, and in practice, it usually includes the lead-up and preparation of analyses, reports, presentations, and arguments that will influence the outcome.

3.3 Information Security Metrics

There are many different aspects to managing information security risks and, hence, many different elements that could be measured.

Compared to fields such as financial and operations management, metrics in information security are relatively immature. Few organizations have a coherent suite or *system* of information security metrics in place, and hardly any would claim that their security metrics are comprehensive. A surprising number of organizations still don't use any at all! Others use a bewildering array of security metrics with little if any consensus on what generally ought to be measured—a core set of essential information security metrics, if you will. Worse still, while several sources list things that could be measured, nobody really agrees on *how* to go about choosing or developing metrics that are appropriate for a given organization: there is very limited guidance on the process of selecting or developing appropriate metrics and, in some cases, dubious pseudo-scientific advice about the methods of collecting, analyzing, and presenting data.

Context is important: many of the information security metrics that are appropriate for your particular organization may differ from those needed by others, even your peers in the same industry. The process for determining the metrics your

organization actually needs (discussed in detail in Chapter 8) can be summarized by thinking through who needs to know what, when. In other words, measurements are made to provide information supporting managers and operational people in making decisions. Measurement information has to be relevant and meaningful to the recipient. Anything else is just noise.

We have no knowledge of your specific situation, so our advice has to be generic, but where possible, we will provide realistic examples to help you apply the tools and techniques to select suitable metrics.

3.4 Financial Metrics (for Information Security)

During the past decade or more, a variety of approaches have been developed in the effort to improve security metrics. Along the way, financially based security metrics spun away from the mainstream on something of a tangent of their own.

In *Managing Cybersecurity Resources: A Cost–Benefit Analysis*, two well-respected professors of economics and accounting* address the rhetorical question, “How can you know if your firm is committing too much money, or not enough, to protect itself against such unseen hazards?” (Gordon and Loeb 2006). The answer, apparently, involves a conventional cost–benefit analysis using standard accounting methods, such as net present value (NPV) or internal rate of return (IRR), to appraise investment options. In Gordon and Loeb’s highly rational world, managers justify and select certain cybersecurity projects purely on the basis of their net value (benefits less costs). While the cost part of the equation is *relatively* straightforward, the benefits of security require some creative thinking using techniques such as ALE and SLE:

- Annualized loss expectancy (ALE) is simply the anticipated average annual loss from security failures, projected in line with the losses that have accumulated in the preceding years. Simply stated, if you have suffered historical losses totaling, say, \$28,000 over a 10 year period, and you anticipate the same level of loss to occur over the next 10, then the ALE is \$2,800. There are major assumptions inherent in ALE.[†] For a start, it is assumed that someone has been accurately identifying and diligently recording the costs of security incidents: if not, the ALE is pure guesswork. Second, it is assumed that you have enough knowledge and understanding of the situation (meaning the risks—the threats, vulnerabilities, exposures, and impacts) to predict the

* We suspect professors Gordon and Loeb might be a little embarrassed at being billed as “global leaders in the critical area of cybersecurity” in the book’s marketing blurb. It is pretty obvious from the way they use the term “cybersecurity” and refer to the Internet as if it had only just been invented, that they have nontechnical/non-IT backgrounds. We decline to say whether that represents a benefit or a cost.

[†] These are not a million miles away from the theoretical physicist’s “First, assume a spherical cow in a vacuum...”

34 ■ PRAGMATIC Security Metrics

same level of loss for future years as was allegedly experienced before: if not, the ALE is meaningless. Third, ALE implies that information security incidents are broadly similar from year to year in terms of frequency and impact, whereas, in reality, some of the most significant incidents are much more unpredictable. Fourth, it is assumed that such a simplistic financial prediction has some value to management: if not, ALE is a complete waste of time, and you'd be better off heading to the pub for some real ale.

- Single loss expectancy (SLE) is very similar to ALE except that the costs are estimated for each individual event, rather than the cumulative costs for all events during the period. It's still largely a matter of guesswork. The pub is still the more attractive option.

A few financial metrics have also been derived by information security professionals and consultants without necessarily the same depth of immersion in the heady world of economics, accounting, and finance. Two well-known examples are as follows:

- Total cost of ownership (TCO) attempts to predict and quantify the total costs associated with something such as a single security control or perhaps an entire information security management system (ISMS) over its projected lifetime. This approach begs the obvious questions: What is the lifetime for a security control or ISMS? What are the associated costs, and how will they vary during the lifetime? Information security controls are *supposed* to bring benefits that more than offset their costs, but whether TCO takes the benefits into account or merely tracks security expenditure is a moot point.
- Return on security investment (ROSI) is essentially IRR applied to security investments. The basic notion is that if you spend \$1 to reduce losses by \$2, you have realized a 200% return on your investment.* There is a significant difference, however, between measuring the return on an investment in, say, a machine tool and the return on a risk management activity, such as information security: avoiding uncertain future costs is harder to quantify and justify than increasing the profits by a predictable amount. The fluid nature of information security risks makes it impossible for anyone to say, hand on heart, that the security controls have saved *X* dollars, although there is some merit in stating that costs of “at least *Y* dollars” were probably avoided—and so long as *Y* is substantially more than *Z*, the cost of the security controls, the investment is justified. QED.

* Strictly speaking, ROSI accounts for the time value of money, meaning inflation and cost of capital. Given the major assumptions and inherent uncertainties in the projections, whether you factor it in using IRR, NPV, or “payback period” makes no odds in practice because these erudite accounting considerations are overwhelmed by the sheer guesswork involved in estimating the value of security incidents that will be avoided. We're pragmatists, remember.

Tip: As far as we are concerned, the jury has been out a very long time on the value of financially based security metrics. Despite the involvement of some talented academics, the end goal has thus far proven rather elusive. For what it's worth, we do believe in building conventional business cases for security investment and improvement projects, theoretically comparing the projected net financial position up to a year or three after the project completes against the projected net financial position if the project doesn't take place (the null hypothesis). ISACA's Val IT method (see Section 3.5) holds real promise in terms of both building better business cases and generating better metrics to squeeze every ounce of value from a project's output.

3.5 (Information Security) Risk Management Metrics

The management of risk is an expansive and important field of study and practice, not least because it takes in the management of financial risks. The *outrageous* bonuses earned by successful traders, especially in the highly leveraged world of futures and options, stem from the *obscene* profits that trading firms can make from even small unit gains on huge trading volumes. As we have seen recently, financial risk has its downside, too. The economic meltdown that triggered a global recession resulting from bad credit risks, which, in turn, were accepted through bad risk management decisions coupled with distinctly dubious governance, management, and accounting practices all topped off with a sprinkling of corporate greed.

Risk metrics, then, are enormously significant for the financial services industry. The entire insurance market, for example, owes its very existence to risk metrics and statistics, that is, projections made on the basis of statistical analysis of historical data. Calculating acceptable levels of risk is an essential part of the competitive and sustainable pricing of insurance cover.

With respect to information security risk metrics, specifically, another tangential spinoff effort has been quietly developing the practice of *quantitative information security risk management*. Its proponents dangle the prospect of *objective risk analysis* in front of management, and indeed, there are objective, quantifiable, even scientific elements to their methods. Given sufficient historical data, it is feasible to make projections reliably, with statistically valid confidence limits or bounds to reduce management's uncertainties and stomach ulcers. But did you spot the key assumptions in that statement? Aside from needing *sufficient* historical data (which is a significant issue in a practice as young, immature, and dynamic as information security), quantitative methods are still attempting to predict the future on the basis of the past, implicitly assuming that we should expect more of the same (the very antithesis of dynamism). Business cases for information security investments built on so-called objective risk models should probably say at the bottom, "Past

performance is no guarantee of future results. The value of your investments may fall as well as rise, and you may not get back the money you put in.”*

Despite our apparent cynicism, we accept that there are circumstances in which quantitative risk analysis has merit, meaning we don’t completely discount the value of quantitatively derived risk metrics. Part of our reasoning is that, as information security grows up, we are gathering more and more data, meaning our predictions are gradually becoming more fact-based. At the same time, the slow maturity of information security metrics means we are not just collecting greater quantities of data but more relevant and better quality data.

3.6 Software Quality (and Security) Metrics

We honestly don’t have the space to do this important topic justice here, but we encourage you to explore it at your leisure. Measurements are a *big deal* both for modern software development and for the IT systems they produce. Numerous major research studies have investigated and evaluated different approaches for measuring and managing projects, spawning a mini-industry of development methods and quality assurance practices. There are *methodologies*,[†] guidelines, and standards aplenty, including a bunch covering the information security aspects of software development. In among all that activity there are lots of hints about the importance of metrics and ideas on how to measure stuff.

A paper concerning the quality of eCommerce systems (Stefani and Xenos 2009) merits a specific mention because it uses the term “metametrics.” The authors proposed 10 metametrics or parameters for selecting suitable metrics, the first five of which had been introduced previously (Olsina and Rossi 2002):

1. *Measurement scale*: for example, nominal, ordinal, interval, ratio, and absolute
2. *Measurement independence*: the ability of a metric to generate the same result when measured by different types of users
3. *Automation*: a measure of the effort required to measure the metric using a tool
4. *Simplicity*: a measure of the clarity of the metric’s definition
5. *Accuracy*: does the metric actually measure what is supposed to be measured?
6. *Cost*: the cost of gathering, analyzing, and using the metric
7. *Evaluation*: the type of measurement process
8. *User type*: the kind of user involved in the calculation of the value of a metric
9. *Target*: does the metric measure data or processes or both?
10. *Persuasion*: the extent to which the metric is associated with desirable quality characteristics

* We quite like the idea of ending that with “Seek competent professional advice,” but we’re not *certain* that exists.

† Whatever happened to common or garden methods? Do we really need an -ology?

Tip: When thinking about the way metrics are designed and used, why stop here? Aside from the specific areas we have mentioned so far in this chapter, metrics are used in almost every field of human endeavor. Look out for numbers, statistics, and graphs as you go about your daily life. You'll see them on TV, hear them on the radio, and read about them in newspapers and magazines. As you do, ponder the quality of the metrics: which metrics are good, which are bad, and what determines the differences? We will return to metameetrics specifically in the information security context in Chapter 6 et seq.

3.7 Information Security Metrics Reference Sources

A small but growing body of literature* means that we are far from being the only sources of information and guidance on information security metrics. We are happy to acknowledge the excellent work of other authors, thought leaders, and experts in the field on whose shoulders we stand, and in turn, we encourage them and you, dear reader, to criticize and build on what we offer here. It may be nice to receive positive feedback and glowing reviews, but informed, critical comments and rational improvement suggestions tend to be more helpful in driving professional practices forward.

Information security metrics comprise a tiny and (some would say) inconsequential corner of the much bigger field of metrology, the science of measurement. Metrology, in turn, is but one narrow aspect of mathematical science. To gain a full appreciation of information security metrics, a visitor from Alpha Centauri would have to start with the works of Avogadro, Newton, Hertz, Pascal, and a million others, not all of whom have units of measurements named in their honor. In terms of reviewing and commenting on other works, we had to draw the line somewhere when writing this book, so the brief outlines below are limited to information security metrics resources.[†]

3.7.1 Douglas Hubbard: How to Measure Anything (Hubbard 2010)

While *How to Measure Anything* concerns measurement in the context of business management in general, risk is a central theme throughout the book and IT

* For a far more thorough survey of the security metrics literature, see Barabanov (2011).

[†] Please excuse the negative bias in our reviews that follow: it's not that we disrespect the authors in any way (quite the opposite), but our *perception* of errors and omissions in the published security metrics literature was largely what inspired us to write this book. You may vehemently disagree with our opinions, but either way, we encourage you to read and carefully consider all the resources described here if you are serious about information security metrics. We are not writing in isolation but contributing to the existing body of knowledge. The context is important.

security examples illustrate the approach. The author's thesis is that the purpose of measurement is to reduce uncertainties (risks) in decision making. With that broad perspective in mind, estimation is a perfectly valid and useful way to measure things that are impracticable or impossible to measure otherwise. Statistical techniques such as Monte Carlo analysis of complex multivariate situations, plus the "calibration" of people to counteract the natural tendency to be over confident in assessing risks (see Appendix K), leads to more accurate and precise estimates, i.e., better measurements. By encouraging managers to approach difficult issues such as measuring and managing IT security, investment, marketing and project management risks in this manner, Douglas has opened the door to more creative and scientifically valid metrics."

3.7.2 Andrew Jaquith: Security Metrics (Jaquith 2007)

Security Metrics is promoted as a comprehensive guide to security metrics best practices. The coverage is certainly broad, ranging from the mathematical considerations underpinning metrics to their use in measuring technical security elements, such as antivirus and application security, and managing security programs. Jaquith's final chapter on designing security versions of the Balanced Scorecard (Kaplan and Norton 1996) is as challenging as it is helpful. The original Balanced Scorecard used a handful of metrics on each of four *perspectives* (financial, customer, internal business processes, and learning and growth) as a decision support tool for corporate performance management. Jaquith proposes modifications of the perspectives to suit security management (e.g., changing the customer perspective from that of customers of the business to internal customers of the security function) and suggests a selection of metrics for the altered perspectives. Although he is reasonably explicit about the proposed changes, readers are encouraged to consider and adapt the suggestions to suit their circumstances rather than simply follow a generic menu.

Jaquith is a prolific, highly regarded, and influential writer, widely acknowledged as a guru in the field of security metrics. He writes in a forthright style that appears to discount, perhaps even discredit, alternative approaches and opinions that he clearly disagrees with, and as such, he has, at times, led the field down a narrow, somewhat introspective path. His strident descriptions of good metrics, bad metrics, and nonmetrics, for example, have perhaps unwittingly constrained the professional dialogue to number theory and statistics. According to Jaquith, metrics must be expressed as a cardinal number or percentage, not with qualitative labels such as "high," "medium," and "low," and expressed using at least one unit of measure, such as "defects," "hours," or "dollars." We consciously favor a more practical, though less academically rigorous, approach reflecting the way metrics are actually being used to measure and manage information security in organizations around the globe. Jaquith is quite right to point out that it *is* mathematically unsound to calculate compound security risk scores using simple arithmetic based

on high = 3, medium = 2, low = 1, etc., but in the absence of a better approach to assessing security risks, such analysis arguably serves a valuable practical purpose.* Traffic-light reports *are* facile, but as a means of focusing management attention on serious security matters, they clearly have a minor but legitimate role in business.

Most of the metrics discussed in *Security Metrics* measure technologies, technical processes, and their inputs, whereas we are more concerned with the management processes and the results or outcomes of information security, in many cases, going well beyond the domain of pure IT security (e.g., we're interested in ensuring compliance with security-related laws and regulations, not just security policies and standards, and business continuity management as a whole, not just IT disaster recovery).

3.7.3 NIST SP 800-55: Performance Measurement Guide for Information Security (NIST 2008)

Billed as “a guide to assist in the development, selection, and implementation of measures to be used at the information system and program levels,” this standard is, in fact, primarily intended for use by U.S. government agencies in support of their obligations under the Federal Information Security Management Act (FISMA). Understandably, the U.S. federal government is quite concerned to find out not only where the nation’s security dollars are disappearing to, but whether they are being spent wisely.

SP 800-55 is remarkably thorough and methodical in just 80 pages. The processes it describes for specifying, developing, and selecting metrics are very similar to those detailed in this book—not because we plagiarized them, but because we converged on a common solution to the same problem. SP 800-55 doesn’t specify PRAGMATIC as such, but it does recommend selecting a set of metrics for initial implementation that have certain qualities. It even mentions scoring and weighting them. It just doesn’t go as far as to say how to do that.

The executive summary states, “the following factors must be considered during development and implementation of an information security measurement program:

- Measures must yield quantifiable information (percentages, averages, and numbers);†
- Data that supports the measures needs to be readily available;‡

* Classifying security risks and then analyzing their distribution across the classes or categories, calculating trends in the distribution, etc. are mathematically sound and valid calculations because the item counts are cardinal numbers. Jaquith himself might accept that pointing out the fallacy of applying ordinary arithmetic to ordinal numbers has led to some security professionals shying away from ordinals completely, which is an (understandable) mistake, one we don't think he intended to suggest.

† Shades of Jaquith (2007).

‡ Available only to authorized and legitimate requestors, we trust!

- Only repeatable information security processes should be considered for measurement; and
- Measures must be useful for tracking performance and directing resources.”

The standard refers to three categories of measure:

1. Implementation measures (“used to demonstrate progress in implementing information security programs, specific security controls, and associated policies and procedures”)
2. Effectiveness/efficiency measures (“used to monitor if program-level processes and system-level security controls are implemented correctly, operating as intended, and meeting the desired outcome”)
3. Impact measures (“used to articulate the impact of information security on an organization’s mission”)

SP 800-55 identifies just 19 “candidate measures”—an admirably brief short list of metrics that is acknowledged to be not comprehensive and in need of tailoring to suit each agency’s measurement requirements.

3.7.4 Debra Herrmann: Complete Guide to Security and Privacy Metrics (Herrmann 2007)

In this heavyweight textbook, Herrmann details *more than 900* security metrics. The book is particularly strong on measuring compliance with North American laws and regulations relating in different ways to security (e.g., GLB, SOX, HIPAA, PIPEDA, FISMA, and NERC CIP), taking up a quarter of the 800 pages (!), but there are still many pages left to discuss technical and physical security metrics and even a few on financial security metrics. Chapter 2 gives a decent general introduction to the development of metrics using the goal-question-metric paradigm. Herrmann states, “good metrics are accurate, precise, valid and correct.”

The 900+ metrics would be completely overwhelming if presented as an unstructured list, but it helps that they are individually introduced and described in context. Herrmann says, “No organization should attempt or even could implement all of these metrics and still accomplish its mission or return a profit. Rather, this collection should be considered like a menu from which to pick and choose metrics that will be meaningful to your organization; most likely, the metrics considered useful will change over time due to a variety of factors. Often there are subtle differences in the way the data is analyzed and presented from one metric to the next in the same category. It is up to you to decide which are the appetizers, entrees, and desserts, and whether you want the low-salt or the spicy version.”* Hear hear!

* At one point, we toyed with calling this *The Security Metrics Cookbook*. Because it neatly complements Herrmann’s book in many respects, that might actually have been an apt title.

3.7.5 W. Krag Brotby: Information Security Management Metrics (Brotby 2009a)

Brotby's experience and expertise in security management and governance account for the high-level/managerial—as opposed to low-level/technical—focus of the book. He starts, for instance, with a very brief overview of *performance* metrics used to operate technical security controls, but delves deeper into financial, quality, and business approaches to measuring security that are probably unfamiliar territory for many security professionals. If you are simply looking for advice on firewall statistics, this is probably not your ideal reference, whereas if you want to manage information security more effectively across a complex network, it's right up your street.

Being one of the authors of the present book, there is bound to be a lot in common with Brotby's previous book on this subject. However, aside from Gary Hinson's involvement, Brotby's own thinking has developed since writing the earlier volume, and indeed, the whole field of security metrics continues to evolve. Arguably the book's most valuable contribution to the field is its description of the attributes of good security metrics and the concept of ranking metrics. Brotby's eight key attributes (manageable, meaningful, actionable, unambiguous, reliable, accurate, timely, and predictive) directly inspired the PRAGMATIC approach we shall soon describe here.

3.7.6 Lance Hayden: IT Security Metrics (Hayden 2010)

Possibly as a result of his academic background and perhaps limited work experience, Hayden discusses security measurement mostly in the context of *security improvement projects* by which he means discrete project activities to improve some specific aspect of IT security. He also refers several times to *security measurement projects*. Projects tend to be discrete work packages with defined project managers/leaders, budgets, starting points, end points, and goals. Information security management does involve some IT security projects or initiatives, but a significant amount of effort and resources are directed toward running and managing ongoing security operations. These operational activities may not have a specific manager/leader and often have rather indistinct, diffuse, presumed, or simply undefined security goals. It is not entirely obvious how to apply Hayden's advice to the derivation of security metrics supporting routine information security operations.

Like Herrmann (2007), Hayden favors the goal-question-metric (GQM) approach to document the security goals for a project, draw out related questions that are being addressed, and then identify possible metrics. Unfortunately, he mostly skims right past the critical project initiation and definition activities that would normally allocate the project manager/leader, set the budget, determine the starting and ending points, and, most of all, define the goals or outcomes required of the project: these are, of course, vital activities in relation to the quality and nature of security the project is to deliver.

IT Security Metrics is well written and well worth reading, particularly in relation to defining worthwhile metrics for security improvement projects.

3.7.7 Caroline Wong: Security Metrics: A Beginner's Guide (Wong 2012)

With practical tips and useful notes throughout, Caroline's book is admirably easy to read, although we are unsure whether it is aimed at beginners to security metrics, or beginners to security, perhaps both.

The book is strong on project management metrics, taking account of social factors when presenting metrics, and technical design of an enterprise wide XML metrics database system. There are plenty of suggestions on prioritizing security activities.

Caroline's focus on automated data collection and aggregation for large enterprises over emphasizes operational IT security metrics over strategic, non technical and 'soft' measures – a bias shared by many security professionals from IT/technical backgrounds.

Despite the promising heading "Decide What to Measure", Section III (Chapters 5 and 6) offers little advice on *how* to identify what needs to be measured and select worthwhile security metrics. Chapter 5 "Identify Core Competencies" concerns IT security competencies, outsourcing of security and the performance of technical security activities such as changing firewall rules. The few metrics suggested here are labeled "quantitative" (e.g., "Percentage of patches deployed within the time-frame specified in the information security group's service level agreement") or "qualitative" (e.g., "Which business units receive network vulnerability scan reports from the information security team?"). Chapter 6 "Identify Targets" talks about measuring security things that are important (e.g. compliance and risk), broken (security processes or technologies that might be improved), basic (immature parts of the information security program), worth discussing (issues of interest beyond the security team) or new (costs and functional requirements for new technologies).

We are puzzled at Caroline's interpretation of "qualitative metric": the examples she offers are mostly questions that would generate lists of items (such as "Who has access to the system?") or binary answers (such as "Does this technology integrate with third party partners or providers?") rather than the kinds of numeric measurements that are generally considered to be metrics. Questions of this nature are more commonly associated with IT compliance audit checklists than information security metrics."

3.7.8 ISO/IEC 27004: Information Security Management–Measurement (ISO/IEC 27004 2009)

ISO/IEC 27004 is a member of the ISO27k family of information security management standards produced by an international team of experts under the auspices of the International Organization for Standardization (ISO) and the International

Electrotechnical Committee (IEC). The standard is intended to help organizations measure, report on, and, hence, systematically improve the effectiveness of their information security management systems.

It “provides guidance on the development and use of measures and measurement in order to assess the effectiveness of an ISMS and controls or groups of controls, as specified in ISO/IEC 27001. This would include policy, information security risk management, control objectives, controls, processes and procedures, and support the process of its revision, helping to determine whether any of the ISMS processes or controls need to be changed or improved.”

The standard has the following key sections:

- Information security measurement overview
- Management responsibilities
- Measures and measurement development
- Measurement operation
- Data analysis and measurement results reporting
- Information security measurement program evaluation and improvement

Annex A of the standard suggests a template on which to describe a metric, and Annex C offers some worked examples.

The standard is quite detailed in terms of the mechanics of measurement processes. It laboriously describes how to collect *base measures*, use aggregation and mathematical calculations to generate *derived measures*, and then apply analytical techniques and decision criteria to create *indicators* used for ISMS management purposes (i.e., metrics, although the term is meticulously avoided for some arcane reason). Unfortunately, it does not offer much guidance on *which* base measures, derived measures, or indicators might actually be worth all this effort and gives only the merest hints about how users might select their own.

3.7.9 CIS Security Metrics (CIS 2010)

In November 2010, the Center for Internet Security published a *consensus* set of ~28 security metrics definitions* developed by a team of 150 industry experts who set out to create “a collection of unambiguous, logically defensible outcome and practice metrics measuring: the frequency and severity of security incidents; incident recovery performance; and the use of security practices that were generally regarded as effective.”

The ~28 metrics do not cover the entire information security metrics landscape but are technology-centric, covering certain aspects within IT security. Each metric is specified in a standardized and explicit manner (in the style of a technical specification for a software function or perhaps an electronic component) and is

* Only 27 metrics are described in detail in the CIS paper. “Number of incidents” is mentioned though not actually specified, but—hey—we can take a stab at that one ourselves!

accompanied by paragraphs briefly describing its objectives, uses, and limitations, plus references. This gets a little tedious and repetitive, particularly for simple metrics, such as “Number of Applications,” which takes a page and a half to describe. However, because the metrics are intended “to be used across organizations to collect and analyze data on security process performance and outcomes,” the specifications are explicitly detailed in order to encourage consistency and comparability between organizations. Unfortunately, although the initiative seems to have kept going, there does not appear to be an active forum for sharing CIS metrics as such, but if you are prepared to help, you are invited to join the team.

As with most other lists of security things that can be measured, there is precious little attempt to justify the selection or really explain the value of the chosen metrics to readers. The development team’s discussions around each metric are not provided or summarized, for example. We don’t know why or on what basis these particular 28 metrics were selected from the dozens that we suspect would have been considered and rejected. Why would you want to measure *cost of incidents* and *mean cost of incidents* separately, for example, when both are derived from the same base data? There *may* be legitimate reasons for including these two metrics separately, but if so, we are left in the dark.

3.7.10 ISACA

Just in case you are not already familiar with it, ISACA is a longstanding professional membership organization, originally* serving IT auditors but latterly extending its tentacles into the related fields of information security management, IT governance, and IT risk. Its Web site is www.isaca.org.

The COBIT method (ISACA 2011) started out in the 1990s as a tool to help IT auditors plan and conduct IT audits by systematically deconstructing the key activities and controls pertaining to the IT department. In the course of the intervening 15 years, it has evolved into a more comprehensive IT audit management-focused tool, picking up the *best practices* mantra along the way. The current incarnation of COBIT, branded now as an IT governance framework and supporting toolset, is much more polished but still incorporates the structured breakdown of IT management and operational functions.

The Val IT method (ITGI 2008) draws heavily on the groundbreaking approach pioneered by John Thorp concerning getting the most value from IT investments. “Measuring the things that count” is a key feature of Thorp’s benefits realization approach, one of the “three necessary conditions” eloquently described in his book.

* This was way back when IT was known as electronic data processing (EDP), computers had rows of flashing ping-pong ball lights and toggle switches, and whirring banks of tape drives, and the best-dressed EDP guy wore a white lab coat and glasses, sporting a clipboard under his arm and a propelling pencil in his coat pocket. And yes, Admiral Grace Hopper aside, EDP pros in the advertisements were *always* guys. These were indeed pre-PC times.

Tip: If you can find it, buy *The Information Paradox* (Thorp 1998), read it, and pass it on to the CIO...but first photocopy Chapter 7 for your private study as you will probably never see your book again.

Chapter 7 details how to design a good measurement system, select suitable measures that measure the right things in the right ways, and use those measures to guide management decisions. Although Thorp's context was financial management of IT projects, the concepts apply equally to information security management.

Business Model for Information Security (BMIS) was developed as a systems approach to the subject (ISACA 2009). It is represented as a visually striking 3D pyramid with six *dynamic connectors* linking the four nodes (Figure 3.1).

The model pitches information security as a dynamic, interconnected system, all the component parts interacting with and so influencing each other. With that precept, it is necessary to understand the various elements of information security and how they interconnect and interact in order to understand where the issues

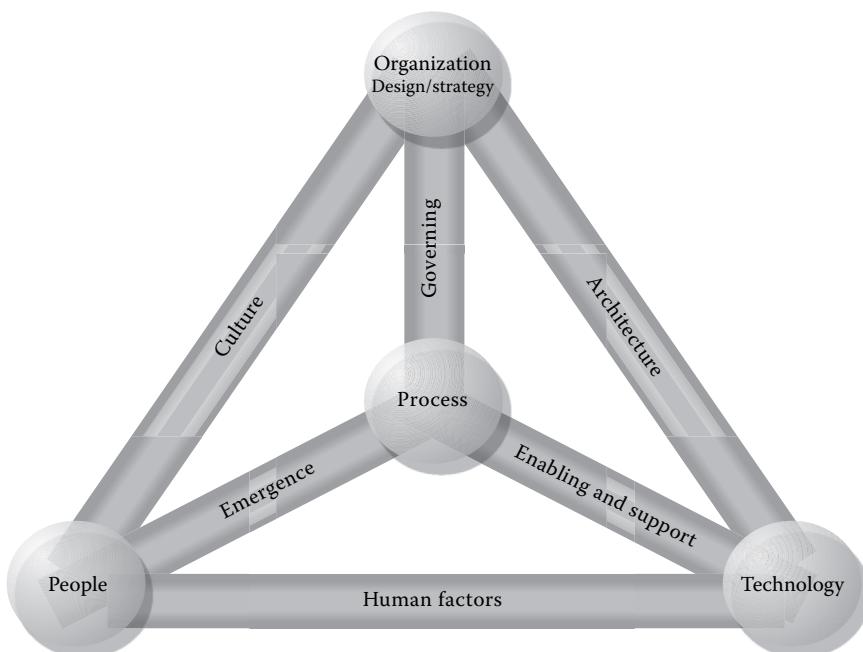


Figure 3.1 Business model for information security. (From ISACA, *An Introduction to the Business Model for Information Security*, 2009. With permission.)

might be and, hence, address them. BMIS therefore offers a structured way to analyze the objectives of security management and, hence, security measurement. For more on BMIS, see Appendix B.

Guideline G41 “Return on Security Investment” (ISACA 2010) states, “Security metrics are measures designed to facilitate decision making and improve performance and accountability through collection, analysis and reporting of relevant performance-related data. Security metrics focus on the actions (and results of those actions) that enterprises take to reduce and manage the risks of loss of reputation, theft of information or money, and business discontinuities that arise when security defences are breached. Primary considerations for development and implementation of a security metrics programme include the following:

- Metrics must yield quantifiable information such as percentages, averages and numbers.
- Data supporting metrics must be readily available.
- Only a repeatable process must be considered for measurement.
- Metrics must be useful for tracking performance and directing resources.
- Metrics should not be expensive or laborious to gather.

3.8 Specifying Metrics

The *raison d'être* for information security metrics is to support decisions and actions relating to information security goals, which, in turn, relate to desired business outcomes, as illustrated in Figure 3.2.*

To define and develop worthwhile metrics, the intended audiences, therefore, need to reach consensus on outcomes and then intermediate or related goals that support or enable those outcomes to be reached. As the outcomes and goals are further defined and elaborated on, important aspects or parameters generally become apparent until eventually possible metrics start to crystallize.

The process can be structured and formalized in various ways, for example, using BMIS, COBIT, ISO/IEC 27002, and other structured frameworks to consider all aspects while determining which factors and elements of information security are sufficiently important to warrant being measured.

A popular approach described by Hayden (2010) and Herrmann (2007) is called goal-question-metric (GQM). GQM was developed for software engineering. The method essentially involves three steps: (1) identify organizational goals, (2) identify questions relating to the component parts and activities needed to achieve those

* Our figure is adapted from Hauser and Katz (1998): we simply added the information security goals.

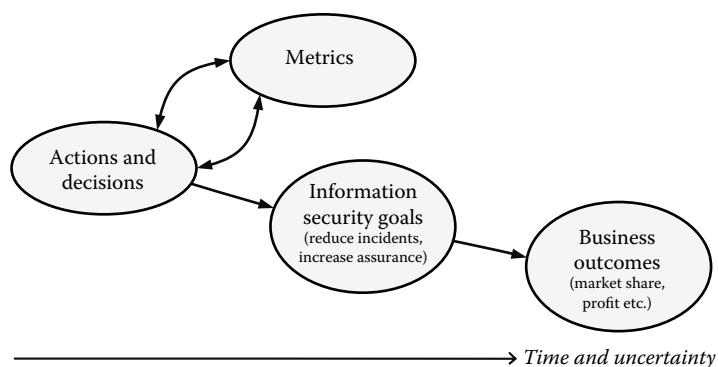


Figure 3.2 Information security metrics support business outcomes.

goals, and (3) identify metrics to address the questions. It sounds simpler than it really is, but like many things, it gets easier with practice.*

Another straightforward approach, again from the software engineering field, is the Capability Maturity Model® (CMM)[†] originally developed by Carnegie Mellon University as a way to improve the quality of software development practices (Paultk et al. 1995). CMM defines a series of five levels describing common practices that are characteristic of each level. An information security version of the CMM would look something like this, in outline (a more complete version is provided in Appendix C):

CMM level 1: Ad hoc: information security risks are handled on an entirely informal basis. Processes are undocumented and relatively unstable.

CMM level 2: Repeatable but intuitive: there is an emerging appreciation of information security. Security processes are not formally documented, depending largely on employees' knowledge and experience.

CMM level 3: Defined process: information security activities are formalized throughout the organization using policies, procedures, and security awareness.

CMM level 4: Managed and measurable: information security activities are standardized using policies, procedures, defined and assigned roles and responsibilities, etc., and metrics are introduced for routine security operations and management purposes.

CMM level 5: Optimized: Metrics are used to drive systematic information security improvements, including strategic activities.

* We demonstrate the use of GQM to develop a metric for the VP marketing in the case study/ worked example in Chapter 12.

[†] Capability Maturity Model is a registered service mark of Carnegie Mellon University.

In CMM, key process areas (KPAs) characterize each level, and within each KPA are defined goals, commitment, abilities, measurements (hint!), and verification.

3.9 Metrics Catalogs and a Serious Warning about SMD

After working a few years in information security, information security professionals often feel the urge to get into security metrics for a very practical and obvious reason: we desperately need them in order to manage information security properly. We start to look around at what metrics other people are using and maybe come up with one or two of our own. Reading this book, you probably have a few ideas already. We have some, too. Before long, we find ourselves idly composing little lists of metrics on odd scraps.

If you find yourself at this point, *beware*. There is a real danger that you, too, might be coming down with security metrics disorder (SMD). We've mentioned some of the early warning signs already, but trust us, there's worse to come.

You know you've caught SMD when

- You not only Google “information security metrics” again, but this time, you get beyond the first page or so of results.
- You become strangely attached to certain metrics, referring to them as *my* metrics.*
- You join metrics groups intending to participate in the discussion and boast about *your* metrics but immediately get distracted by bright shiny new metrics to play with.
- You feel a compulsion to share *your* metrics with other people, but *they* don't seem quite as excited about them as you are.[†]
- You feel curiously deflated at discovering someone else is already using one of *your* metrics and thoroughly disheartened when you realize they are using several.
- You decide it's time to aggregate your metrics lists and notes into a little black notebook[‡] and start hunting for all those odd scraps.

* Sociologically speaking, isn't it interesting that we feel we “own” certain metrics? Maybe it's something to do with the personal intellectual investment and creativity involved in coming up with a novel metric or the buzz we get when we think about all the fantastic things we can achieve with it. The buzz is addictive: SMD is an addictive disorder.

[†] If you notice them jotting down notes about the metrics you mention, they probably have SMD too, but they may not realize it yet.

[‡] Some of us take that literally, picking up an actual book in which to keep metrics notes, while others compile documents on our computers. Chronic SMD sufferers prefer pocketbooks that we can take with us wherever we go or park in the little room for those private daily moments of peaceful contemplation.

- You catch yourself compulsively checking through security metrics catalogs (revealed by other sufferers of SMD) to see if they have got *your* metrics.*
- While perusing other lists, you not only spot lots of interesting new metrics but you *add them to your little black notebook*, and so your list grows.
- You worry about how to structure your list in order to make sense of your growing collection, so taxonomy raises its ugly head.
- You think about exactly which fields you would include in a metrics database and in what order.
- You have an inkling that the only person who will never be satisfied with the *information security measurement system* is you.
- You see *everything* in terms of metrics, measurements, data, analyses, reports, and graphs. You see numbers everywhere, even where there are none (zero, nil, 0). Hallucinating slightly, you start to feel awash in an ocean of statistics, experiencing an overwhelming feeling not unlike being seasick.
- You wonder which would be the best metametrics and whether anyone else has thought of metametametrics.
- You search Amazon, ostensibly to find good books on security metrics but end up searching the reader feedback comments for yet more metrics.

Those are the symptoms of the acute phase. Although there is no known cure for SMD, you may find some relief with other distractions that help take your mind off security metrics—an absorbing hobby maybe or quantitative risk management. Chronic sufferers of SMD actually *do* compose metrics databases, inventories, and catalogs. Some of us publish them and invite others to contribute (mostly, it has to be said, so that we will pick up additional metrics).† We discuss the best way to reference our metrics and postulate global standards for security metrics schemas.

Ultimately, we write books on security metrics, thereby infecting the next generation of SMD sufferers with the meme. Sorry. Help is at hand: Join the SMD club at www.SecurityMetametrics.com. Just remember to start every posting with something like, “Hi, my name is Gary, and I’m a metroholic.”

3.10 Other (Information Security) Metrics Resources

For an even wider perspective on metrics, measurement, statistics, and so forth, see the bibliography (Appendix L), browse a good science/business bookshop, or search the Web for still more reading materials. The www.SecurityMetametrics.com Web site supports and extends the information in this book, and we welcome your involvement. We maintain a Web page of annotated hyperlinks to metrics

* Naturally, you have already pored over *our* metrics catalog, having immediately turned to Appendix F, right?

† And yes, patently, we *have* thought about metametametrics. We still are. We’re a lost cause.

50 ■ PRAGMATIC Security Metrics

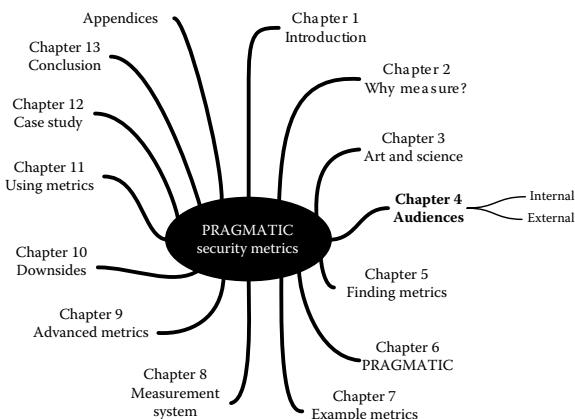
resources elsewhere on the Internet—it is obviously easier for you to click a link than to type it in, especially as things are always changing on the Web, and URLs are distinctly ephemeral.

3.11 Summary

This chapter was our attempt to relate information security metrics, specifically, to the broader field of metrics and measurement generally.

Chapter 4

Audiences for Security Metrics



The quintessential group interaction is to break the large group into smaller discussion groups. It forces the participants not only to think about your message but also to connect and collaborate with others and to apply the new information.

It also inherently increases the energy level!

Kristin Arnold

We will shortly go shopping for candidate information security metrics, but first, let's consider who we are shopping for. Who will need them? And, literally, who will pay for them? It is important that we think through who the audiences for our metrics

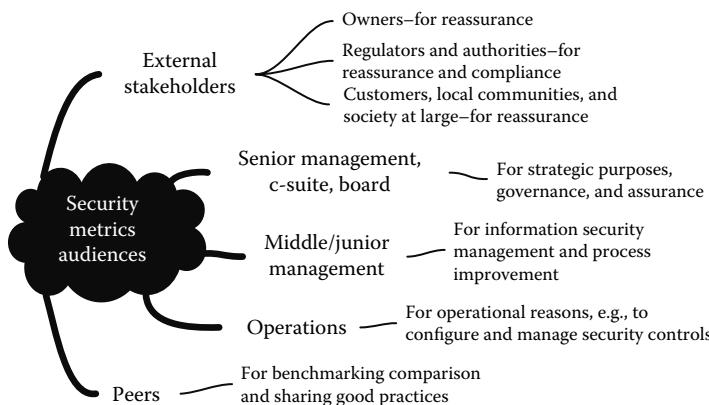


Figure 4.1 Key audiences for information security metrics.

are because they are the customers, consumers, or users of the measurement data, stakeholders in the *information security measurement system*, and as such, they have requirements that, in due course, the system will ultimately be designed to satisfy.*

The mind map/diagram (Figure 4.1) outlines five distinct audience groups.

Notice that the audiences shown at the top and bottom of the diagram are external to the organization, whereas the management and operations functions shown in the middle are within it. We will talk about the insiders first.

4.1 Metrics Audiences *Within the Organization*

A great place to start the job of specifying information security metrics is to figure out *who* does *what* in relation to information security within the organization.[†] This sets the stage, clarifying what management information will be needed to support key decisions. Unfortunately, security-related roles and responsibilities are not always entirely obvious—they are not usually fully and explicitly documented in job descriptions and don't necessarily reflect the formal organizational chart. It may therefore be prudent, as part of the process of implementing information security metrics, to remedy this issue by mapping out roles and responsibilities, delineating as unambiguously as possible who is supposed to be “doing security.” Clarifying the accountabilities for the protection of information assets, generally through the nomination of information asset owners, is

* We will be exploring *measurement systems* in some depth in Chapter 8. It's an important concept, but, for now, let's simply assume that we are trying to select security metrics individually without much regard to the bigger picture.

[†] We are, of course, blithely assuming that *someone* accepts responsibility to do the finding out! Are you reading this book simply out of a genuine interest in the topic, or have *you* been asked to sort out the security metrics? Either way, good luck!

especially beneficial and has significant advantages elsewhere in the information security program. *Understanding the audiences' key concerns will help enormously in determining which aspects of information security are of most direct interest and, hence, what kinds of security metrics are worth short-listing.*

4.1.1 Senior Management

Perched on top of the tree, senior managers and company directors have the widest field of view and the heaviest accountabilities. Their primary role is to determine and set the organization's overall strategies, and they have governance responsibilities to put the resources, structures, systems, and processes in place to deliver the strategic objectives, plus the reporting mechanisms to find out what's actually going on at the lower levels of the hierarchy.

Aside from all that internal corporate stuff, senior management also acts as a point of contact for external stakeholders (such as shareholders/owners, regulators, and other authorities) while most strategic objectives are outwardly focused on the markets for the organization's products and competitors.

Information security is clearly just one of many important issues on senior management's plate. Senior management defines security strategies and policies that will work alongside other business strategies and policies. Two other aspects that tend to put security on senior management's agenda are compliance and risk. In governance terms, senior management is expected to ensure that the organization adequately complies with security-relevant laws, regulations, and contractual obligations and has major security risks under control alongside myriad other risks. Senior managers are likely to be held accountable for serious compliance failures or breaches and for serious security incidents that impact and devalue the corporation. At the same time, senior management has to juggle risk against reward: while taking on too much risk could be deemed reckless, it is also counterproductive for the organization to be excessively risk-averse because that hamstrings the business and unduly constrains its capabilities and opportunities.

Regarding senior management's requirements for information security metrics, they need high-level information to build up the bigger picture but don't usually have much time to delve into details. The most obvious demand is for metrics relating to the organization's information security strategies and initiatives along with information on its compliance and risk status. Less obviously, but equally importantly, senior management needs assurance that things are under control. A simple all-clear on security makes an admirably succinct management report, but what if security issues are either being deliberately withheld from them or are not even appreciated by lower levels of management?

It can also be useful to put yourself in the shoes of people in various roles to consider whether candidate metrics are of any use to them in performing their tasks.* For instance, if you were to become CFO or even CIO for a day, would you

* We used exactly this approach to develop the worked example in Chapter 12.

be interested in how many packets the firewall dropped yesterday? Somehow, we doubt it! It's more likely that you would want to know the extent of losses and other impacts from security incidents and whether the ongoing expenditure on security controls is justified in relation to other funding demands. In a heavily regulated industry, compliance with obligations imposed by statute, regulators, or contracts are bound to be of concern to senior management, so measures of compliance with key controls (including relevant information security controls) are likely to figure quite high up on senior management's wish list.

4.1.2 Middle and Junior Management

The routine management of information security normally falls to middle or even junior managers, in particular, someone designated as the information (or IT) security manager, although as security awareness gradually reaches the upper echelons, organizations are increasingly appointing more senior chief (information) security officers to oversee information and physical security.

Given that the profession is still evolving, it is often somewhat unclear what the information security manager is or, rather, should be responsible for. Information security responsibilities elsewhere in the organization are seldom concisely or precisely defined either.

While clarifying security responsibilities is a vital stage in the development of a mature information security management program, this is no trivial undertaking. Ensuring there are designated owners for security policies, exceptions, and exemptions, for example, is gospel, but organizational politics being what they are, it is not unusual to find significant resistance from many quarters to this kind of endeavor. Accountability for information security is a corporate governance issue. Once people realize security incidents will reflect badly upon them if they were expected to protect the information assets impacted, they are naturally reluctant to accept responsibility. Hence, as is so often the case, success depends on senior management buy-in and support; otherwise *they* may be held to account for failing to protect the organization's information assets.

Even when responsibilities and accountabilities are fairly well defined on paper, there remains the issue of finding powerful individuals who are well entrenched, lurking semi-submerged deep within the guts of the organization. We are talking here about the notion of *nexus of influence*.^{*} For various reasons, certain individuals have influence above and beyond what is immediately apparent from their formal job titles or positions in the organization. While it's usually *glaringly obvious* to

* There are fairly straightforward ways to discover who these individuals are. The analysis may even be automated to some extent: because there is a correlation between those who have the most lines of communication and those who have the most influence, a forensics product called FBI from Australian company Nuix examines the mail servers to generate an influence map based on the amount of email traffic between various individuals.

other insiders who *really* wields the power in an organization, it may be worth digging deeper to establish this more scientifically. In relation to information security, for example, who does the following?

- Is often consulted or asked for his or her opinion on things and is listened to whenever he or she speaks up?
- Signs off on or approves things and, conversely, has the power to block or stonewall things?
- Originates or proposes projects, initiatives, and, in a broader sense, organizational changes?
- Calls and leads meetings?
- Is always the first to know stuff?

The exercise of identifying which individuals within the organization (and, for that matter, outside it) have the most influence over information security has a dual purpose. You have the opportunity not only to garner their support for the security metrics work but also to understand their information needs and sources. Identifying and ideally interviewing them or those around them can be a fascinating and worthwhile exercise if you have the time and sufficient support from senior management to open the necessary doors.

Another possible approach is to explore prior management decisions that have been made regarding information security, especially anything that appears controversial or odd. If a record exists of historical decisions adversely affecting security, this may offer insight into some of the metrics that need development to guide management into coming to more appropriate conclusions. For example, if the organization deliberately goes against the grain by, say, refusing to assess information security risks systematically or to classify information resources, find out how such decisions were made, when, and by whom.* Speak to anyone who has failed to get a security project or budget approved, not about the merits of the specific project/budget, but about the decision-making process. Try to determine exactly what information was provided to the ultimate decision makers, by whom, and in what format. Was any information presented that directly challenged the proposal? Might certain *hard data* have changed the outcome?

4.1.3 Security Operations

Most medium-to-large organizations these days have at least some people (either on the payroll or under contract) whose job relates directly to securing or protecting information and other corporate assets. We're talking about the security administrators, network/systems security analysts, security guards, security architects, and

* With 20/20 hindsight, it may even turn out that the metrics presented were inadequate, failing to provide sufficiently meaningful information for the decision to come out otherwise!

Tip: Developing security metrics makes a decent team project. The information security manager *may* be best placed to specify strategic and management-level metrics but also may not necessarily be, and he or she is probably no longer as in touch with things at the operational level as he or she once was. The particular personality traits that equate to an uncanny talent for spotting metrics opportunities and identifying killer metrics are not entirely restricted to more senior security people.* Juniors may need some assistance to appreciate the bigger picture, perhaps an introduction to the PRAGMATIC approach, but on the other hand, their naïveté is an asset with respect to questioning the meaning or sense of metrics that seem intuitively obvious to, say, the information security manager! It's not a bad idea to involve security contacts from the wider business, too, because their perspective is likely invaluable.

* They also suggest an increased risk of catching SMD.

so forth. They need information about security risks and controls in order to install, configure, run/operate, and tweak the security machinery. These people may truly need to know how many packets were dropped by the firewalls yesterday or how many spams were blocked. They also need a range of information to ensure that security policies, procedures, guidelines, and standards are properly implemented and are effective in practice.

Most juniors in any field have aspirations of climbing the ladder to more senior positions. Security metrics help junior information security professionals appreciate that they are important cogs in the bigger machine. This may seem a trivial point, but think about it: isn't one of the most rewarding and motivational aspects of *your* job knowing that you are making a difference—that your work is genuinely appreciated?

4.1.4 *Others with Interest in Information Security*

They may not think of themselves as information security professionals, nor may they report to someone who does, but various other people in the organization do “security” things or have an interest in information security. We just mentioned security contacts distributed around the organization. Other examples include the following:

- Backup operators
- Other governance, risk, compliance, and control experts/specialists
- Internal auditors and other assurance and assessment specialists

- Business continuity, disaster recovery, contingency planning, and related specialists
- IT professionals, generally, plus anyone designing, developing, configuring, using, managing, and maintaining IT systems (yes, that's a lot!)
- Anyone handling information (yes, that's practically everyone!)

Aside from any specific needs for particular metrics to perform particular security-related tasks, some information security metrics have general value in connection with the security awareness program. Take, for instance, a metric such as the number of information security incidents last month: It may not be especially useful as a management or operational metric, but as a simple tool to remind employees in general about information security, it has potential.

4.2 Metrics Audiences From *Without* the Organization

Most of us who consider security metrics at all are thinking about their use within the corporation, for internal strategic, management, and operational purposes, but that's not the end of it. A number of external stakeholders have an interest in the organization's information security status and so are also potential audiences for certain information security metrics.

Take customers for example, particularly customers who have provided valuable information, such as credit card numbers, or those who are reliant on the organization to supply the products they have ordered (e.g., in various forms of outsourcing). It is perfectly reasonable for them to expect the organization to protect their information and to be able to fulfill their orders, so in that sense, they have a stake in the organization's information security and business continuity.

The same may apply to suppliers and business partners, especially in tightly integrated business-to-business supply networks. Information security obligations may be explicitly imposed on the organization through contracts and agreements or by laws and regulations.

Regulatory bodies, government departments, business partners, and others may insist on reviewing, inspecting, or auditing the organization's security and continuity arrangements, meaning they clearly have an interest in the organization's security status. If a trustworthy and proactive organization were to supply them with a steady stream of security metrics (provided the metrics are credible and reflect reality—e.g., if they record security incidents and security improvements), they might gain confidence in the way it is managing information security, perhaps enough not to need as many security reviews, inspections, and audits. Those are, of course, techniques for measuring security; hence, the PRAGMATIC approach has value.

An even broader but less well-defined audience consists of business prospects and contacts (not necessarily current customers, partners, or suppliers, perhaps those just evaluating your products and considering a purchase) and, in a sense,

Tip: Dividing the total audience into groups such as those we have described above implies that each group is homogeneous, whereas, in fact, it is composed of individual people with, to some extent, unique information needs and communications preferences. It is not usually practicable to design and produce custom reports to suit individual recipients, but occasionally, that does make sense (e.g., a one-on-one presentation and discussion with a senior manager on an information security topic of direct concern to him or her). More generally, it is worth making information security metrics accessible to people with a range of communications preferences by, for example, incorporating visual images (such as graphs and other graphics) as well as written words, descriptive text, as well as lists or tables of numbers, and making in-person presentations as well as delivering written reports.*

* There is more advice along these lines in Chapters 11 and 12.

society at large. Which would you trust more: an organization that is confident enough in its information security arrangements to describe them and disclose security metrics versus one that is secretive and evasive on security matters?

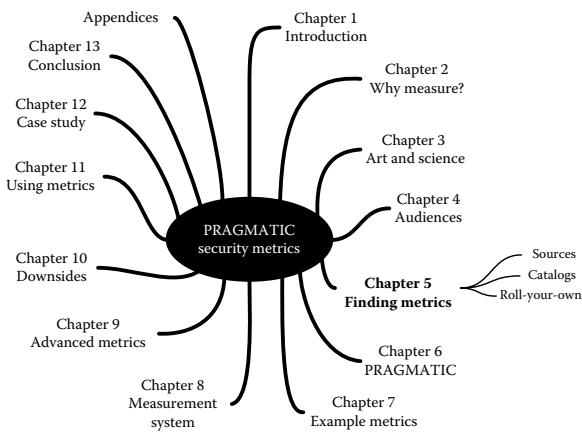
Furthermore, we rely on a wide range of public and private organizations supplying or supporting critical national infrastructure services, not least our governments. Wouldn't it be good to know that they are in good shape, information security-wise, and can be trusted to look after our interests? PRAGMATIC metrics can help here, too.

4.3 Summary

This chapter explored the surprisingly wide range of people or bodies with an interest in information security metrics. Dividing the total metrics audience into discrete segments rather than amorphous blobs such as “management” is worth the effort in that different audiences generally have different information needs. The division between internal and external audiences is particularly significant. This approach becomes vital when we move on to design a coherent *information security measurement system* later (in Chapter 8), and yet there are times when it is appropriate to divide the audiences all the way down to individuals.

Chapter 5

Finding Candidate Metrics



What gets measured gets done, what gets measured and fed back gets done well, what gets rewarded gets repeated.

John E. Jones

A few pages ago, we mentioned there is no shortage of things that could be measured in relation to information security. Anything that changes can be measured both in terms of the amount and the rate of change and possibly in other dimensions as well. Given the dynamic and complex nature of information security, there are a great number of things we could measure. As this chapter will soon show, it's really not hard to come up with a long list of potential security metrics, all candidates for our *information security measurement system*.

Tip: “Well-instrumented systems monitor and measure only those elements that are useful or essential to the required management tasks. Assuming a determination has been made of critical activities and the potential for serious impacts and tolerance for risk, then the issue of effectiveness must be considered in terms of the necessity for certain specific types of information” (Brotby 2009a).

For our purposes, the trick will be to find those things that both (1) relate in a reasonably consistent manner to information security, preferably in a forward-looking manner, and (2) are relevant to someone in the course of doing his or her job, in other words, they have purpose and utility for security management. We will tackle that issue shortly through the PRAGMATIC approach, but first, in order to help you identify candidate information security metrics that are right for your situation, this chapter offers some advice on where to go looking for inspiration. Along the way, we are deliberately going to lead you astray from the well-beaten path to explore the ways other fields, besides information security and IT, choose and use metrics.

5.1 Preexisting/Current Information Security Metrics

Very few information security managers ever have the luxury* of a green-field opportunity to implement the perfect set of information security metrics completely from scratch. Especially if you are relatively new at this game and your organization has been into information or IT security for some while, your existing security metrics may be a little lackluster or thin on the ground. There’s no shame whatsoever in that: you have probably bought this book in order to improve your security metrics. You might not have been involved when the current crop of security metrics were first developed—it’s quite common, in fact, to find that some data are routinely collected, processed, and reported, although *nobody* can recall exactly why! Nevertheless, your existing security metrics do provide a platform, a starting point, and some of them may well feature in due course in your more mature *information security measurement system*.

This book provides the tools to evaluate your existing security metrics to determine which of them are truly valuable enough to be worth keeping. Retiring security metrics that are no longer deemed sufficiently valuable will cut costs directly and bring other indirect benefits, such as simplifying management reports, making them more focused and less “noisy.”

* Would it truly be a luxury or a challenge? Discuss.

Tip: Take a long, hard look at your existing information security metrics—more than just a cursory glance. Perhaps even draw up an inventory listing all the metrics along with their key characteristics (such as source, destination, and reporting frequency). Don't forget metrics that are gathered, used, or reported less often or sporadically. For starters, have you reported anything to anyone in the past week? What numbers did you present? Where did they come from? Aside from whatever you reported to others, what numbers did you use yourself? If you are truly inspired by this book, you will find that your inventory expands markedly over the next few months both in terms of the number of metrics and the details recorded. A simple list or spreadsheet will suffice for now.

5.2 Other Corporate Metrics

Aside from information security metrics per se (i.e., measurements that are collected specifically or primarily for information security or IT security purposes), all organizations collect, analyze, report, and use many others. Because information is the absolute lifeblood of management, metrics comprise one of the most important categories of data flowing within the corporation. Not all information security metrics necessarily belong to, or are generated and used by, the information security department. Any actively trading medium-to-large-sized organization will be awash with a huge number of metrics, a lot of which are potentially of interest for information security:^{*}

- *Risk management* typically maintains a risk register of some sort, which (we hope!) ranks risks that could be classified as information security risks in comparison to various others.
- *Physical/site security* typically maintains statistics on security guard rostered hours while managing the card access and other security systems that have their own built-in reporting capabilities.
- The *help desk* can amass a great deal of information that may be eminently useful regarding user problems, incidents, etc.
- Most *IT departments* are awash with metrics, many of which could be classed as information security metrics. System uptime and statistics on outages, for instance, may be tucked away in the voluminous appendices of service-level performance reports, and performance and capacity management revolves

* Many general business management metrics may appear to have absolutely no information security relevance at first glance, but don't be too hasty: they may correlate with or validate other relevant bits of information and may well have significance even if apparently oblique or orthogonal. Aside from that, *all* metrics are fascinating, aren't they?

around numbers: these are directly related to the availability of information. Change, version, patch, and release management systems are a treasure trove of security metrics, not forgetting statistics from the problem and request ticket/tracking systems used by the IT help desk on password resets, access requests, etc. Operating systems and management utilities pump out data on aspects such as loading, performance, and capacity (highly relevant to availability) and *security events* such as logons, software errors, and system faults tucked away in various system/audit logs.

- *Legal/compliance functions* maintain records and reports on requirements mandated by applicable laws (e.g., privacy), regulations (e.g., SOX), and contracts (e.g., payment card industry–data security standard or PCI-DSS). Some of them are directly security relevant; others are less so.
- *Internal audit* has an interest in information security, particularly concerning the organization’s core financial systems. Is anyone tracking the number and severity of IT audit findings or checking that IT audit recommendations are completed by their due dates?
- The *finance department*’s bean counters are legendary! Pretty much anything with a dollar sign attached tends to involve the finance department in some way. At the very least, there are probably line items for the information security department’s annual budget and expenditure somewhere, and—trust me—when discussing information security matters with senior management, it helps to have more than just a vague idea of the organization’s gross capital, turnover, and profitability.
- The *human resources department* ought to know how many employees there are, what jobs they are doing, and how much they get paid, so it ought to be easy to figure out how much is spent on the personnel side of security, right? OK, maybe not, but it definitely should be able to tell you the headcount for information security management and site security (assuming they exist as discrete functions, of course).
- In the same vein, *procurement/accounts payable* ought to know how much is being spent on security products and services, including “security consultants”...
- *Sales and marketing/accounts receivable* records the number and value of customer contracts and tries hard to assess the value of the organization’s brands: this is fantastic news for a hard-pressed information security manager trying to put figures on the potential costs and other impacts of serious security incidents and disasters.
- *Business continuity management* (BCM) maintains and helps the business develop and tests its plans and preparations to cope with disasters. Look to the BCM people for a conceptual map of the organization’s critical business processes along with an overlay showing the IT systems and services supporting them, plus metrics regarding BCM plan status, coverage, and test results.

- *Operations management* maintains all manner of data and statistics about the production processes, including a raft of data used to configure and control machine tools in the factory and, generally, data from the machine tools, supervisory control and data acquisition (SCADA), and statistical process control (SPC) systems concerning their operations. Service industries are no less well instrumented, for example, call center operations amass mountains of data about calls handled, waiting times, and so forth. They might also be able to gauge customer sentiment, such as hostility toward the organization, which could certainly have security implications.
- Many *business applications and processes* generate security-relevant data, such as the number of forced match transactions recorded by the procurement system, plus overrides and exceptions in general.
- *Senior executive and nonexecutive management* is accountable, overall, for corporate governance. Part of that involves knowing what is actually going on down in the greasy bowels of the boiler room—not in detail but clearly enough to find out about substantial risks and serious issues that could adversely affect the organization as a whole. That, in turn, means senior management is obliged to put in place the reporting and directive processes necessary to discover risks and control operations accordingly. These days, “I had no idea what was going on” is a very lame excuse. Just ask any board member roughly how many pages they are expected to consider in the average board meeting for some idea of the vast stack of metrics routinely sent to senior management (leaving aside all the other papers, reports, emails, and texts that never make it onto the official agenda).

Provided you don't suffer from the IT-myopia that typically afflicts professionals who refer to themselves as “IT security specialists,” it's obvious there is an enormous wealth of security-relevant metrics readily available throughout the average organization. While most of the management information coursing through the organization's veins would never be called “information security metrics” as such, it can often provide relevant inputs or information for security management with just a little lateral thinking.

Aside from the question about what things are being measured, the measured data values may have information security implications. Significant changes in key corporate measurements sometimes—arguably often—signal security risks

Tip: Expanding your field of vision to find out what metrics are used elsewhere in the organization can reveal a cornucopia of potentially useful information, as well as opening your eyes to new measurement techniques, reporting styles, etc. When you step outside your office, don't be surprised to find other metrics experts out there. We are not alone.

that might need to be addressed. An unexpectedly high or low rate of change of employee turnover {metric 8.3},* for example, clearly implies that *something* is going on, but is it a risk? Could it have an impact on security? Is it significant? Is a competitor headhunting staff in an effort to elicit sensitive information, perhaps, or are disgruntled and resentful employees escaping the clutches of an overbearing or sexually harassing boss? A little deductive reasoning or investigation might conclude that if the hump is caused by the loss of employees from the super-secret product research and development group, it's probably the former. If the analysis points to attractive young ladies exiting in droves from one particular department or team, it might well be the latter. Either way, this ostensibly nonsecurity metric may just have revealed a security situation that otherwise would have remained hidden under the cloak of corporate politics.

Here's another example. IT change requests are often handled—and recorded—routinely by the IT help desk. One of our suggested metrics {metric 10.4} reconciles IT change requests to system configuration changes, information that should be logged and available from IT. "What does this measure?" you might ask. Well, compliance for one thing: are there changes taking place that didn't follow the change and configuration management process? That sounds like a procedural problem, and it may well have security implications. Tracking the metric over time may show whether the information security program is headed in the right direction, especially if coupled with metrics covering other aspects of compliance. Sampling activities selectively in this manner may not give an absolute measure of security compliance but can nevertheless be a good indicator of the overall compliance picture. And because these are relatively easy measures to gather, they can be performed regularly, often even, whereas compliance checks are usually only performed infrequently by the auditors and the odd diligent and concerned manager.

Other examples of information that can serve as measures, metrics, or indicators for information security include the following:

- *Departmental and project budgets and expenditures:* by themselves budgets may not be too relevant, but if compared to prior periods, they may be useful indicators of change (e.g., upscaling or downsizing). Significant budget cuts are likely to be accompanied by stress and, possibly, layoffs, which is likely to translate into increased risk. Significant increases in budgets may mean many new hires and initiatives, which can also introduce added risks. Substantial overspends may result in urgent budget cuts elsewhere, and substantial underspends may release funds for opportunistic security activities.

* We use this notation to reference information security metrics examples explained and scored in Chapter 7 and listed in the master table of metrics in Appendix F. The first part of the reference number is the applicable section number from ISO/IEC 27002 and, hence, indicates the primary purpose of the metric. The second part is a serial number. SMD strikes again.

- *Strategies, plans, and proposals*, perhaps to the level of business cases, action plans, and diaries of key events: most significant organizational activities will have implications for information security. The information security manager should try to get on the distribution list for major proposals, etc., in order to find out what's coming up, ideally in time to get involved in the planning but at least to be able to respond more effectively if it's approved.* Well-written business cases and plans contain even more information to analyze in terms of potential risk and impacts.
- *Statistics from security systems*, such as network probe, spam, and malware numbers from firewalls, anti-spam, and antivirus systems, respectively. These are the traditional security metrics that can be useful to the extent that they provide operational information to those managing these devices and systems. Rolled up, they also tell us if the machinery is performing properly or if decisions need to be made to beef up these capabilities.
- *Post-incident review reports (PIRs)*: incidents can be very instructive in the sense of being truly unplanned tests of our security[†] and, hence, can provide exceptionally useful measures. They identify the things we've overlooked or missed (e.g., previously unrecognized or unappreciated risks, inadequate or missing controls, lack of adequate monitoring or metrics) and can serve to remind everyone of the importance of the security function. Thorough no-holds-barred PIRs or independent postmortems help enormously in uncovering the true root causes, providing a very firm basis to justify necessary security improvements. They can even identify security controls that worked effectively, preventing an even worse disaster from occurring! All it takes is an enlightened management that appreciates that those who don't learn from history are destined to repeat it and has the fortitude to set aside the objections from those who whine about airing dirty laundry in public.
- *Audits and security reviews*: properly conducted, audits and security reviews can uncover risks and potential problems before an incident serves to point them out. Even if, in practice, most audits are under the purview of finance and so the information security manager is not included in the process, efforts should be made to get access to audit reports at least. Much of what is

* Business types, especially those who may grudgingly tolerate IT or site security but are decidedly uncomfortable with the subversive notion of information security, may query the desire of security to review these materials. Best be prepared to provide a viable rationale and reassure management that the information is in safe hands. This situation is a strong argument for appointing a chief information security officer as a senior management role that is *expected* to get involved in major strategic decisions.

[†] Why is it that most organizations only consider conducting post-incident reports on serious incidents that affect them directly? How about learning from minor incidents and from incidents that affect third parties, too? Near misses even! Gain the benefits without the impacts. This, to us, seems to be one of those things that are blindingly obvious once stated, but think about it: what does *your* organization do? What about the places you've worked before?

Tip: In our clumsy, roundabout way, we are hinting at data mining—essentially finding previously unrecognized patterns and relationships in large databases, thereby revealing unexpected additional information of relevance to information security. Data mining is *way* more advanced than information security metrics, but if you are looking for a serious new challenge, the field is wide open.

uncovered by financial audits will have significance for information security. Tracking audit reports, findings, ratings, and recommendations over time can provide a useful set of metrics.

Our search for good metrics will likely be more productive if we broaden our horizons beyond conventional wisdom to look at what's changing around us in the organization, both qualitatively and quantitatively—maybe try some “what if” analysis to determine how changes in all sorts of things might, in some way, affect some aspect of security.

5.3 Metrics Used in Other Fields and Organizations

Turning now from the corporation's internal management information and metrics to the outside world, let's first consider how many fields of endeavor besides information security and IT use metrics.

Any number of disciplines can be considered models for metrification that we can potentially apply, or at least adapt, to information security, particularly well-established fields and practices such as engineering (especially safety-critical engineering), sports (yes, sports: remember Roger Bannister's four-minute mile? What a guy! What a metric!), medicine (e.g., epidemiology, the study of population health), meteorology (not to be confused with metrology, it's the real science behind the TV weather presenters), logistics (including navigation), and, in fact, all branches of science and mathematics have long since developed the key principles of measurement or metrification. They are all actively using and benefiting from metrics. Sectors that are more mature than information security typically have far better ways to measure and keep track of things, which is why they are more mature.

We needn't reinvent the wheel.

It can be productive to discover the sorts of things measured in other fields and find out how they do it. Extensive experiences in, for example, the measurements necessary to operate trains and factories have homed in on specific measures that work and discarded those that did not. Procedural compliance when operating, say, a nuclear power plant or a hospital is an absolute requirement, so gaining insight into what management does to ensure procedural compliance may prove inspirational. You might perhaps talk to an airline pilot who also has an endless gamut of

procedures and checklists to follow when busily checking parameters and metrics on the flight deck: metrics failures in this context can have dramatic consequences; hence, the reliability of metrics goes right back to basic aerospace engineering and design principles.*

Your organization's competitors and business partners, especially your peers in the information security profession, undoubtedly face very similar information security challenges as you do. We are all dealing with essentially the same threats and often the same vulnerabilities.[†] In short, we have a lot in common, including the need to manage and improve information security. Professional membership associations, such as SANS, ISSA, or ISACA, provide the opportunity to mix with and pick the brains of peers on what they are doing about metrics, although, because you have made it this far already, it's likely your brain is the one that will get picked! Nevertheless, if you keep your eyes open and your ears peeled, meetings, seminars, conferences, courses, trade shows, and other gatherings—including webinars, blogs, discussion groups, and other virtual venues—are all good sources of inspiration on which security things to measure plus hints on how to measure them.

5.4 Information Security Metrics Reference Sources

Several books, standards, and articles, including those we mentioned in Section 3.7, focus on security metrics. Most of them either lay out variously categorized lists of suggested security metrics or weave a bunch of metrics into the text. Appendix E lists more than 140 Sherwood Applied Business Security Architecture (SABSA) security attributes and identifies possible metrics for each of those attributes. Searching the Web for “information security metrics” gives literally millions of Google hits at the time of writing.[‡] In addition, as if that's not more than enough already, we will shortly present and score 150 information security metrics examples using the PRAGMATIC method. We may be flogging a dead horse here, but clearly there is absolutely no danger of ever running short of security things to measure.

Metrics have been of increasing interest to a number of professional organizations in information security for a few years now, though it is fair to say that we are *years* behind our engineering, science, and similar colleagues. Most have suggested certain information security metrics, although mostly in the technical arena, and a few of them score reasonably well against the PRAGMATIC criteria described in Chapter 6.[§]

* We'll pick up that thread in Chapter 9.

[†] White, gray, and black hats alike! Obviously, we don't all share identical perspectives and objectives, but we're all playing the same game, dancing around the same handbags. Even hackers have their security metrics!

[‡] www.lmgtfy.com/?q=information.security.metrics.

[§] Generally, they don't score very well, but then ours *is* a novel approach, and we're all paving the same path.

Tip: Don't be misled into thinking that just because certain metrics have been suggested or recommended by well-known, trusted, competent professional bodies, such as SANS, ISACA, ISF (Information Security Forum), CIS (Center for Internet Security), NIST, OWASP (Open Web Application Security Project), OCEG (Open Compliance and Ethics Group), CSA (Cloud Security Alliance), and ISO/IEC, or fine authors such as Andrew Jaquith, Lance Hayden, Debra Herrmann, George K. Campbell, or indeed ourselves, they must be good. None of us, not one, knows your unique situation in enough depth to propose specific security metrics that will definitely work for you. We don't know what security issues concern your management today. We can barely guess what sources of raw data you have available or can get your hands on at a reasonable cost. We have no idea what security metrics you might already be using or have tried before and how the security metrics are intended to fit into the entire corporate suite or system of metrics. On the other hand, reference sources may well suggest metrics that turn out to be useful or point you in directions that you can explore further. Treat them as prompts for consideration, not gospel. These are candidate metrics, not appointees.

Whether any of the security metrics suggested by external reference sources are directly suited to *your* security measurement requirements is for *you* to decide. We wrote this book largely out of our personal dissatisfaction with the metrics commonly proposed, the feeling that there *must* be better information security metrics, and, most of all, the desire to explain how to go about identifying and selecting better metrics.

If you are feeling completely overwhelmed by all this, don't worry. We will soon explain how to short list and select "a few good security metrics" (Berinato 2005) using the PRAGMATIC approach and then how to weave your chosen metrics into an *information security measurement system* that will knock the spots off most of your peers.

5.5 Other Sources of Inspiration for Security Metrics

5.5.1 Security Surveys

Numerous organizations release surveys on nearly every imaginable aspect of information security, particularly IT security, but often touching on related areas such as governance, risk, and compliance. Some of the more popular and reliable surveys that we're aware of are produced regularly by respected organizations, such as PwC, KPMG, Verizon, Aberdeen, Information Security Forum, PGP/Vontu, ENISA, Ponemon, and IDG.

Tip: Before putting too much faith in *this year's* survey, consider whether *last year's* predictions by the same people were more or less on target or well wide of the mark. In this context, historical performance *is* a guide to the future.

Although it is tempting to just skim superficially through the survey findings over coffee, the better scientifically designed and statistically valid ones are worth studying more thoroughly in order to

- Gain a better appreciation of the context for information security
- Inform and support the development of better business cases for investing in security improvements
- Aid in resource allocation and prioritization
- Examine the data for yourself, draw your own conclusions, and compare your thoughts against those of the survey authors
- Identify trends and spot emerging security issues
- Pick up on generally accepted security practices
- Compare your organization's security status and practices against others
- Find quotable sound bites, pretty graphs, security statistics, informed commentary, anecdotes, and even case-study materials for use in a variety of security awareness, training, and educational materials
- Last but not least, be inspired to come up with novel security metrics

If there is any prospect that you or your management may rely on survey findings for decision support, be sure to read the very boring sections on the survey/sampling methods carefully, for example, online surveys tend to be completed by technophiles; national surveys may not adequately reflect global realities; data, and especially conclusions, in vendor-sponsored surveys may not be entirely trustworthy; small sample sizes and skewed subject-selection methods tend to invalidate the statistics; and changing survey questions may invalidate comparisons with previous surveys.

5.5.2 **Vendor Reports and White Papers**

Vendors of security products (goods and services), along with a few special-interest/pressure groups, release an endless tsunami of reports and white papers. They are mostly glossy marketing tripe that, naturally enough, position the vendors' products as the solution to whatever issues are allegedly identified. If the only tool is a hammer, every problem resembles a nail. Nevertheless, taken with a grain of salt, some of them incorporate or reference interesting and potentially worthwhile statistics, and they may help you see things from different perspectives, which is another source of creative inspiration.

Tip: Built-in security reporting facilities *may* be a good value but only if the things they measure and report actually tell you something you need to know.

5.5.3 Security Software

Most computer programs automatically generate and store performance metadata, that is, information concerning whatever it is that they do, including security. Many provide metadata reporting facilities ranging from crude ASCII text to pretty dynamic graphs and built-in management console displays that wouldn't look out of place on the bridge of the Starship Enterprise. A few even make a decent stab at statistical analysis. Operating systems can generally be persuaded to disgorge performance and capacity information, which is about availability, remember. Security programs, such as antivirus, firewalls, IDS/IPS, access control systems, etc., report things such as the number of security events detected or resolved. In short, as I'm sure we've said before, there is a ready supply of security data if we go looking for it. If anything, we're spoilt for choice.

5.6 Roll-Your-Own Metrics

Although we discuss lots of candidate metrics in this book, we don't purport to know the *best* information security metrics. There are certainly hundreds, probably *thousands* more metrics out there, and, no doubt, some excellent ones yet to be discovered (conceived? invented? conjured up?). In fact, the number approaches infinity if you interpret "information security metric" very broadly and consider every unique combination of metrics as a distinct metric in its own right. The point is that the field is wide open to innovation. If you are creative and willing to give new things a go, you have a golden opportunity to help advance the field by proposing good security metrics whether they already exist in some form (though not necessarily applied to information security, remember) or you come up with them de novo. Provided you are prepared to explain rationally *why* you rate them so highly and what features make them so valuable, there's a fair chance others might adopt them too and a slim chance they might become de facto.

Consider an area most information security managers are not particularly conversant with, such as fraud, and a typical management question,* such as "Where in the organization is fraud most likely to occur?" There are fraud risks everywhere, but the risks are presumably heightened in any department, function, team, or process that involves receiving money (especially cash) or making payments, especially

* Posing the right questions is, in many ways, the art of creating outstanding metrics. Defining measurement objectives is covered in the next chapter.

Tip: Peers and managers will often suggest modifications or alternatives to the metrics you propose, which suggests another approach: instead of focusing on a single metric at a time, why not generate a (small, but perfectly formed) family of related variants and see how they compare?

if the fraud controls are weak. So what metrics might address the question, assuming it has been posed?* The number and value of financial transactions handled might be of interest from the risk perspective. Couple that with some measure of antifraud controls (such as separation of duties) and perhaps incidents (even minor compliance incidents indicating an apparent disregard for the rules), and we are starting to get somewhere. In this case, the information security manager may not have the expertise to design suitable fraud metrics from scratch, but there's a fair chance that brainstorming with colleagues with a fraud or audit background will identify a bunch of candidate metrics to get the ball rolling.

Discussing possible metrics with your work colleagues is one way to weed out the weaklings. If you struggle to explain or justify an information security metric in this friendly environment, you should expect a rough ride if you later report it to management.

5.7 Metrics Supply and Demand

Speaking as reasonably experienced if somewhat jaundiced information security professionals, one of the issues that crop up repeatedly in many discussion forums is that someone naïvely requests metrics for X, whereupon various other members instantly respond with whichever of their pet metrics bears a passing resemblance to X (a matching keyword will do!). The proffered metrics often sound great, not least because the proposers invariably have an overflowing passion for them and can often recount situations in which they were “absolutely perfect.” That enthusiasm is strangely infectious, so the original requestor and, no doubt, others who have observed the exchange add one or more metrics to their personal metrics inventory, and so we continue.

We old farts have been around that particular block far too many times. Our metrics catalogs or inventories are overstuffed. What’s worse, we are still adding to them! The upshot is that we have a ready preponderance of candidate metrics for pretty much any situation you care to name. “Information security risk metrics?” you ask, and we have literally dozens at hand. “Malware metrics for a small

* Framing the key issues sensibly is *crucial* to developing excellent information security metrics. Pretty much anyone can find lots of security things to measure, and most will make a decent stab at addressing management queries using metrics, but posing the appropriate questions in the first place is key.

Canadian company in the medical services industry?” No problem; just give us a moment. Actually, we are past the point of even suggesting information security metrics because others usually beat us to the punch, and at face value, many of their ideas sound just fine.

Eventually someone notices our curious silence and asks, “OK, so what’s the problem, guys? Why *are* you so reluctant to suggest suitable metrics for X? Surely you have some great ideas?” Here is our answer: *Our* pet metrics are our favorites precisely because of the situations we have been through. We are passionate about most of them because we can recall them working brilliantly, solving some management issue that seemed so intractable at the time. Others we may not have used firsthand, but we have pictured ourselves doing so, riding the wave of enthusiasm from another metrics practitioner. It is unlikely in the extreme that the particular situation you find yourself in right now matches one of ours. In suggesting and talking up our pet metrics, we are making *huge* assumptions about your organization, your audience/s, your own metrics expertise, and the metrics maturity of the organization, the information security risks that you face, and the things that concern your management.

That’s why you will usually find us answering the metrics for X question by posing more questions. Who are the metrics for? Why is X so important? What is it about X that needs to be measured? What will measuring X tell you? What do you hope to achieve from the measure of X? What else have you been measuring and for how long? And so on. Our questions seem endless, almost as if we are avoiding the original issue, which, in truth, we usually are.

It is a paradoxical feature of writing this book that we are trying our level best to help you discover the information security metrics that are perfect for you *without* infecting you with our prejudices and passions for our pet metrics, and yet it is those prejudices and passions that led us to search for *the answer* in the first place.*

In our long-winded manner, we are hoping to convince you to start asking yourself, and most of all your metrics audiences, the same kinds of question that we would ask you. We’re trying hard to turn the tide from “Here are some great metrics” to figuring out what it is that your audience/s actually need, changing your focus from supply to demand.

5.8 Summary

Given the distinct possibility that you bought this book in the hope of finding some great information security metrics, Chapter 5 gave you a load of hints on

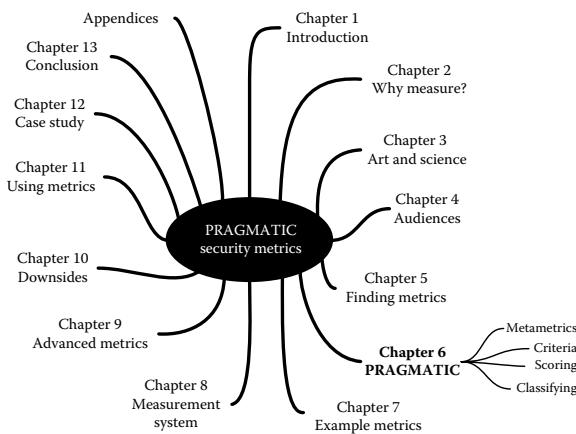
* We are entirely conscious that *some* readers will lap up the example metrics from Chapter 7 as if all their birthdays just came at once. The more sentient ones may consider the scores and the discussion first, but still they will be captivated by the strange fascination that captured us too. It takes a special skill to see a new metric as “just another decision support tool.”

where to go looking, including perhaps a few places that you hadn't discovered for yourself already. Although there are *thousands* of security metrics out there already and well over 150 in this book alone, we even gave you tips on how to create your own bespoke security metrics for that crisply tailored Savile Row look. In the next chapter, we'll give you a tool to make sense of the jumble of metrics, but before you rush ahead, stop and think again about that last section. What is it that you are trying to measure? Why are you measuring it? What will the measures tell you that you don't already know? Because if *you* can't answer those innocuous questions, this book sure as hell can't either.

Free ebooks ==> www.ebook777.com

Chapter 6

Metametrics and the PRAGMATIC Approach



A few well-chosen metrics can be a huge help in monitoring controls and measuring their effectiveness

Clint Kreitner, Center for Internet Security

“A few well-chosen metrics” sounds great! Trouble is, out of the vast range of information security things that we might measure, which ones should we actually select, analyze, and report? To put that another way, *how* do we distinguish good from bad metrics? Which metrics have the qualities we desire? What *are* those desirable qualities, criteria, or parameters, in fact?

It is curious that so little has been said on what we feel is such an extremely important topic. Sure, there are some rather academic reasons why the accountants might prefer net present value over payback period when assessing the projected value of security investments, but in practical terms and in some situations, payback period may have redeeming qualities that make it the more valuable security metric. Other security metrics books belabor the differences between ordinal and cardinal numbers or metrics, measurements, and measures, but few information security practitioners truly understand or even care much about such arcane details, valid as they are. We simply need relevant, useful information in order to manage and deliver adequate information security while our managers and other stakeholders are clamoring for assurance that we have things under control.

The bottom line is that very few organizations today would claim to have effective and comprehensive information security metrics. Security metrics are arguably the capstone for an information security management system,* the final piece of the puzzle that locks all the others firmly in place.

Absent good information security metrics, we are flying blind.

6.1 Metametrics

We define metametrics,[†] like metadata, as information about metrics, including metrics about metrics (e.g., “number of metrics supporting the information security management system” qualifies as a metametric). Metametrics include descriptions of metrics (e.g., most metrics catalogs consist of records for each metric containing fields such as scope, purpose, parameters, sources, and calculations: these are all metametrics). In exactly the same way that information security metrics are used to measure, manage, and improve the security controls and, hence, the security management system, metametrics help us measure, manage, and improve our metrics and, hence, the measurement system.

Metametrics are used

- As indicators of the relative worth or value of each metric when considering various options and choosing the best metrics for the measurement system (see Chapter 8)

* Even ISO/IEC JTC1/SC27, the international committee of highly experienced, competent, and well-respected information security experts responsible for the ISO27k standards, struggles with security metrics. Just look at ISO/IEC 27004 to see what we mean! It's all very well in theory, but how do we actually use it?

† Stefani and Xenos (2009) used the term “metametric” in relation to choosing good eCommerce metrics, noting “Meta-metrics represent different aspects of the measurement procedure like automation, measurement issues and reliability of provided measures.” We have simply contracted the term.

- During tests and periodic reviews of the measurement system to (re)assess the metrics in use, incrementally and systematically improving it (see Section 8.3 phase 8)
- For metrics benchmarking, that is, to compare and contrast metrics with other organizations or between business units in a large organization in order to identify and share good metrics
- To support—and be able to demonstrate if necessary—a professional, rational, and rigorous approach to metrification, which is itself an important part of management and governance

Simply stated, metametrics lead to better metrics.

The heart of the PRAGMATIC method that we will shortly describe involves scoring information security metrics against nine carefully selected assessment criteria, which are, in reality, metametrics.

What might appear at first to be a simple and straightforward metametric—the number of information security metrics you are currently tracking and reporting through your measurement system—is actually quite a revealing example because that rather loose definition could be interpreted in various ways. Do you purely count the number of strategic metrics routinely reported to senior management, or do you include tactical/management/operational metrics and underlying data points that are available for those who want the nitty-gritty? Are you counting data points including historical records or metrics, and can you reliably tell the difference? Such points are clearly important if you intend to measure and track the metametrics consistently over time and can influence the ways in which the metametrics are interpreted by management. The context may be different, but the criteria, issues, and concerns that crop up when selecting metametrics are much the same as those that apply when selecting metrics.

If you design your *information security measurement* system as a discrete activity, the way in which you describe and promote it will often suggest worthwhile metametrics or at least hint at possible measures of the success of the system once it's operational. This is similar to the use of metrics in so-called software development projects, which are usually, in fact, business change/improvement projects with a significant IT element, although that's not such a catchy name! Well-written business cases for development projects lay out the key business objectives for the

Tip: Although we developed the PRAGMATIC method to improve information security metrics specifically, the exact same nine metametrics could be used to assess metrics for other aspects of business management. What's more, with relatively small changes, we're sure it would be straightforward to adapt and apply the metametrics, and hence the PRAGMATIC method itself, for metrics in totally different contexts.

systems being developed, including the projected savings or additional income that will (we hope!) more than compensate for the development costs (see Thorp 1998). Aside from the financial aspects, they also specify key parameters for development, such as the implementation timescales, number of project team members, business man-days allocated, etc. Such factors can be tracked for the development and implementation of the measurement system.

6.2 Selecting Information Security Metrics

Most other books, articles, and standards on security metrics extensively cover rather academic issues in measurement (such as the differences between ordinals, cardinals, and intervals), and some offer lengthy lists of potential metrics. That's all very well for the theoreticians, but unfortunately, they skim through or ignore perhaps the most important issue for security practitioners, offering little if any guidance on *how to determine which security aspects to measure*. We feel it's time to move from theory to practice and fill that void.

The PRAGMATIC approach described in this chapter is an eminently practical method for selecting information security metrics that are workable, useful, and, above all, valuable. In later chapters, we'll demonstrate actually using the method through a number of worked examples.

In the previous chapter, we made it abundantly clear that there is no shortage of information security things that can be measured. What's more, there is no shortage of information security numbers, meaning the underlying raw data. IT systems, particularly security-related ones, such as firewalls and antivirus systems, typically have their own built-in reporting functionality or management interfaces that collect raw data and can crunch the numbers into impressive-looking, full-color graphs for viewing on the console or, these days, as HTML dashboards on the LAN. It is straightforward to capture raw data on various security events from the devices themselves, either through the network or by manual transfer ("sneakernet" or retying the data) into some sort of security metrics/reporting system, ranging in sophistication from basic lists and tables through spreadsheets and databases to full-blown information security management dashboards. In other words, the numbers are readily available. Lots of them.

Availability of data is not the issue here. The problem is *information*. We don't lack things to measure: we lack the means to select the ones that are truly worth measuring.*

* In some cases, frankly, we lack the knowledge, experience, imagination, or the tools to figure out what really matters in relation to information security. Sharing *good* information security metrics, as opposed to simply sharing long, unstructured lists of them, is a way for overburdened security professionals to help each other.

Could you suggest monthly/quarterly reports that I could submit to the management to show how information security in our company is doing? We have standard security appliances like AV, Firewall, SIEM/log management tool, Active Directory, which I could derive reports from. We also have a Patch Management solution & I have these in mind:

1. Virus incidents and how our AV treats them (clean/delete/quarantine)
2. Failed login in our servers, which are being monitored by the SIEM
3. Successful/failed attempts on our firewall

If you have other suggestions, these would be greatly appreciated.

Thanks in advance.

Norman

Above is an absolutely authentic example from the field. The following request was posed on ISO27k Forum, a discussion group for users of the ISO/IEC 27000-series information security management standards.

Norman is considering reporting metrics from his company's antivirus, security information and event monitoring, firewall, active directory, and patch management systems, presumably because these are the security data that are readily available to him. We guess Norman thinks that whoever designed those systems knew the numbers would be needed...so perhaps they are.*

The big unstated question, though, is will those numbers be of any practical use or value to Norman or to Norman's management?

In our experience, senior/executive managers couldn't care less about minutiae, such as how many viruses were quarantined last week. Despite condensing, aggregating, and analyzing the data, quarterly graphs showing the trend in the number of viruses treated are going to be of negligible utility to them. Even junior managers and operational people would, we suggest, only be interested in such specific data items or trends where they relate to specific initiatives, projects, problems, or concerns—for example, if the antivirus system had just been changed to address a problem with its quarantine function. We would class these as *operational data* that can be used to micromanage or fine-tune processes and systems that are already operational. Perhaps the people Norman calls “the management” are at that level?

Managers, senior managers, and executives, in particular, happily leave mere details to their underlings: they are more concerned with the much bigger picture and are generally busy determining and driving future directions for the

* Their metrics capabilities and reporting features were probably mentioned in the systems' marketing glossies and may well have influenced Norman's management to buy them over other—inferior—solutions lacking them.

organization rather than monitoring the breadcrumb trails of precisely how we got where we are today. They mostly assume that security processes and systems previously implemented are running sweetly, doing their thing, and, if not, then operational people ought to be dealing with it *unless* there is something seriously adrift that they need to get personally involved with (management by exception). They may be concerned that different security processes or systems might be worthwhile to address new/different business needs, opportunities, and pressures (particularly legal and regulatory compliance), but their field of vision is (or rather should be!) largely strategic. In a sense, senior managers and operational people look through opposite sides of the binoculars.

Although we have mentioned a broad range of possible information security concerns in previous chapters, they are just examples. Figuring out what *your* managers do actually care about right now in relation to information security in *your* organization and, hence, what information you need to provide today is not something we can do for you. Aside from management's specific information needs, there are other factors to consider:

- Your personal situation, including your role and position in the organization's hierarchy, which affects your own interests/concerns and field of view as well as those of the people to whom you report.
- The state of development or maturity of your information security frameworks, systems, processes, and controls: At a simple level, a newly implemented information security management system is going to be less stable and predictable than one that has been running for years; hence, a 30% degradation in a certain metric may have quite different implications in such different circumstances.
- The personal preferences of you and individual managers, for example, some anticipate report appendices with vast reams of data; some prefer just the highlights but expect to be able to drill-down into the details, whereas others will come back to you or someone else for more information should they need it.
- The state of development or maturity of your security metrics and of management reporting in general.
- Other stuff: managers inevitably have competing demands on their time, so security metrics are inevitably competing with various other concerns and interests for management attention. This is a dynamic factor. If there's a crisis on (even a security crisis!), routine reporting may be temporarily suspended.

If we start planning our metrics on the basis of the data we have readily available from our security systems and processes, it's fairly obvious how they might be gathered/aggregated, analyzed, graphed, and reported. However, there is a significant probability that some, perhaps most, of those reports will be useless to management, meaningless, basically just adding to the noise.

Tip: Metrication is essentially a governance issue. Management should figure out what information it needs in order to find out about, measure, manage, and control the organization effectively. It needs to know that all the important things are pretty much under control, not that something is “at 87.3 trending to 88.4 by next Tuesday.” In other words, *management* ideally needs to pose the questions that the information security metrics will address. We can help them frame the issues and find creative ways to answer the questions, but unless we are managers, we can’t actually pose them.

To elaborate one more time on what we just said, the key problem is not the availability of security-related data but how to select or derive useful, meaningful security-related information that is relevant to management’s needs and helps them make better, more informed decisions, particularly those difficult strategic information security investment decisions—decisions such as the choice between spending a million to generate business that will create significant profits or investing a million to improve security with nebulous, if any, savings. If it was your business and *your* profits, which would *you* choose?

6.3 PRAGMATIC Criteria

It is easy to select a metric; it is hard to select a good metric.

Hauser and Katz (1998)

Our main aim in writing this book is to suggest practical—or pragmatic—ways in which we can pluck out useful, meaningful pieces of information from the turbulent ocean of security numbers in which we find ourselves adrift. Core to the PRAGMATIC method is a comprehensive set of nine metametrics or

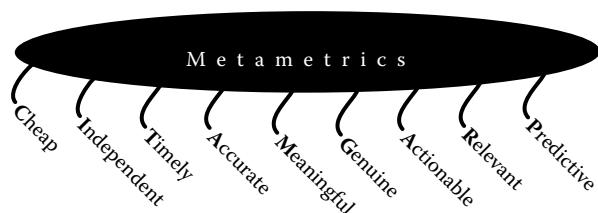


Figure 6.1 Nine PRAGMATIC metametrics.

criteria* for assessing and selecting metrics that, together, construct the acronym (Figure 6.1).

6.3.1 **P** = Predictive

A good security metric is one that **Predicts** security outcomes, implying a causative or highly correlated relationship between the metric and the outcome. The best security metrics predict further and more reliably into the future, and hence **Accuracy** and **Timeliness** are related factors: we'll get onto those shortly.

Lagging or historically based metrics show us what's in the rearview mirror but don't necessarily tell us whether we are headed in the right direction nor what might lie just ahead. Some say sardonically that hindsight is a wonderful thing, but of course, accurate foresight is far more valuable. It allows us to be proactive about addressing information security risks *before* they emerge, giving us the opportunity to forestall, prevent, or, at least, limit incidents. We are talking here about the information security equivalent of quality assurance: getting security *right the first time* (e.g., applying appropriate, proportionate, and adequate security controls) and making it *fit for purpose* (e.g., securing the information assets, systems, and processes that truly need securing, focusing on actual security risks) as opposed to the quality control approach, which involves belatedly discovering and fixing security issues after the fact, that is, following incidents.

Take employee absenteeism levels for instance: high absenteeism could be a result of many factors, such as poor working conditions, better opportunities elsewhere, lax management, poor motivation, bad working practices, etc. It could indicate the workforce's negative attitudes toward the corporation, a dysfunctional corporate culture. This kind of situation could be of concern to the information security manager because of the increased potential for sabotage, information theft, careless data entry, etc., in other words, increasing risks that should perhaps be forestalled now before they materialize. Conversely, low absenteeism (however achieved) could be a sign that employees are more attuned to and aligned with the organization's goals and, arguably, that the associated information security risks are low, so certain internal security controls might be gently relaxed.

Given the number and complexity of factors driving security, reliable leading indicators are hard to find. While there is some relationship, absenteeism is obviously not *strongly predictive* of security. High employee absenteeism might signal the arrival of a major sporting event with next to no security impact other than limited availability of workers! Sometimes we are left with no choice but to settle for predicting or projecting the future using trends based on lagging indicators. The absolute level of absenteeism at any point is of limited value without a meaningful reference or benchmark: the level of absenteeism today relative to prior periods

* From now on, we'll show the initial letters of the key words in bold capitals to remind you that they form part of the **PRAGMATIC** set.

gives us a clue about whether morale might be getting better or worse, information which has some security value and might qualify as a key risk indicator (KRI—more on this to come in Chapter 9).

A bit of brainstorming or creative thinking reveals other potential metrics or indicators along similar lines:

- *Employee turnover*: well-motivated, happy employees are less likely to vote with their feet, and downsizing can decimate morale. Major changes, such as mergers and acquisitions, create enormous anxiety among employees, uncertain if their current roles will still exist in the new order.
- *Number of significant corporate events or changes*, such as releasing new products or entering new markets: increased tension ahead of the event is associated with increased risks and, perhaps, decreased management attention on risk and security matters, while the change that occurs is likely to change corporate risks and, therefore, should be taken into account in the security management system.
- *Corporate growth rate*: rapid expansion, creativity, and innovation in products, etc., are indicative of a successful, effective, happening organization, but at the same time, such rapid and profound changes may open cracks in the corporate defenses. Governance is a challenge at the best of times, more so when the organization is heading into uncharted waters, meaning management has limited prior experience of the risks.

Some of the most useful metrics help us **Predict** things on the basis of identified trends. If we're trending in the desired direction (whatever that might be), it seems likely we're doing something right. A trend is a good example of a relative measure: neither the absolute starting point nor the absolute current value matter, what's important is the rate of change, that is, the difference and the time period between them. Yes, the timescale is part of the metric because (depending on the context) a steep upward movement since the previous quarter probably reflects a markedly different situation from a gradual increase over the past decade. But we digress. Trends are genuine in that it is hard to deny them and harder still to ignore them if they are steep. Trends average out short-term fluctuations to highlight the underlying long-term movement, provided the period over which we average values is not so long as to level significant peaks and troughs.

Here is another way of looking at the **Predictiveness** of metrics. The mind map (Figure 6.2) gives examples of procedural controls that are preventive (i.e., they have their effect before an incident occurs), detective (they come into effect while an incident is in progress), or corrective (they help us deal with the aftermath of an incident). Alongside are some of the corresponding metrics.

While trends can indicate the probable or most likely course, in security, the full range of potential outcomes needs to be considered, including extreme events. Failing to consider true worst-case scenarios leaves us vulnerable to incidents that

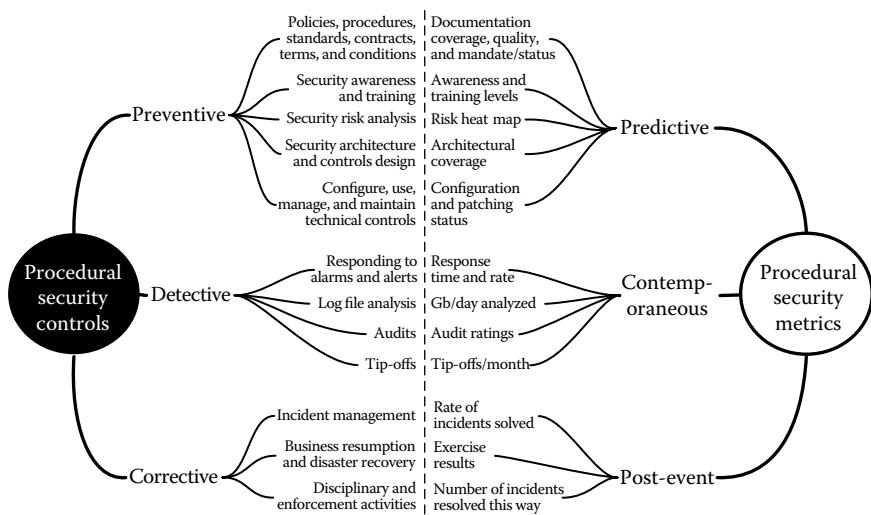


Figure 6.2 Predictive metrics relating to preventive controls.

may be infrequent but tend to be disastrous if (when) they occur.* The key to using trends is not to predict too far, to be conscious of seemingly random fluctuations resulting from the effects of other unmeasured parameters, and to be aware that even with the best of information, events may conspire to create a perfect storm.[†] If you consider all the accepted risks in a particular system and project the consequences if they all materialized at the same time, would that still be acceptable? Insurance risk analysts routinely consider the impact of aggregated risk, but security managers typically don't. The point is whether there exists either a single threat vector that has the capability to exploit numerous vulnerabilities simultaneously or a probability that a number of threats can materialize simultaneously, perhaps exploiting numerous vulnerabilities and resulting in dire consequences. It is this kind of unfortunate (meaning unPredicted) coincidence that creates the perfect storm.

Another rarely considered factor is cascading risk—or more accurately, cascading impact. With today's complex business processes, exemplified by just-in-time

* There may be a physiological basis, a kind of blindness or unwillingness to think the unthinkable—it could be argued that it is a defense or survival mechanism that allows us to concentrate on and deal with more mundane but immediate issues at hand. It could also be argued that if the dinosaurs had seen what was coming, they might still be in charge today. In a few organizations, perhaps they are.

† Ocean waves averaging 20 ft. can, under the right (strictly speaking, the wrong) circumstances, combine to create a so-called freak wave that may be 100 ft. high with potentially catastrophic consequences for any vessel in the vicinity. In a security context, a series of otherwise acceptable risks can, under some circumstances, combine in such a manner that the impacts are truly catastrophic. Good luck if you are hunting for reliable metrics in this arena!

manufacturing techniques that eliminate buffers between steps, the failure of one element or component can cause a domino effect with subsequent elements falling over rapidly as a consequence until the entire process crashes to a grinding halt. The danger is exacerbated by ever more closely coupled IT systems. Although multisystem integration results in higher operational efficiencies, it also increases interdependence and potential impacts in the event of incidents. If the risks cannot be sufficiently mitigated by making the process highly resilient, the only other option may be deliberately reintroducing the buffers, work-in-progress stocks, air gaps, or other forms of compartmentalization. In legacy systems using batch processing or sneakernets, this was not as great a concern, but as processes and systems continue to evolve, this is an area that needs consideration from the information security perspective. Are we becoming seriously fragile? If so, we can confidently Predict problems ahead.

6.3.2 R = Relevant

Of the vast number of security-related parameters that could possibly be measured, we need to focus on those few that provide the most useful information concerning aspects that we truly care about, in other words, metrics that are **Relevant** to the organization's needs. In this context, we can narrow the concept down further to consider management's information needs in relation to controlling and directing information security.

So what information security-related information is most relevant to management? This will be a function of its responsibilities and the decisions it needs to make.

Metrics also need to be reliable and robust, not so much in the sense of availability or simply being there when needed but, more importantly, being reasonably **Accurate**, **Timely**, and **useful**. **Accuracy** and **Timeliness** are separate PRAGMATIC criteria, leaving the utility aspect to be considered further here.

Over time, managers come to rely more heavily on information sources that have proven themselves useful and worthwhile. They tend to focus their attention and respond more rapidly and deliberately to certain metrics than to others.

Unfortunately for us, there are several managers with different personal preferences and needs. We could try to satisfy them all by reporting all their favorite metrics, but that would dissipate the impact of any one metric, confusing the issue still further, and increase our measurement **Costs** unnecessarily. Ideally, we need management to develop consensus on those few metrics that are truly valuable for everyone. One way to do this is through demonstrating their value, which means

Tip: Don't get overly fixated on the numbers. Outcomes are what we are looking for. Relevant metrics are closely associated with achieving desirable security outcomes for the organization, such as reducing risks and increasing compliance, effectiveness, and efficiency.

measuring the value of our metrics through metameetrics. Another way is to get the managers together to thrash out and agree on their common needs, considering the requirements and, in effect, specifying a coherent *information security measurement system* (Chapter 8).

6.3.3 A = Actionable

It's not very helpful to discover from a metric that something is wrong or we're going into the red if we are powerless to do anything about it—all that does is create anxiety. Management must feel it has influence, if not outright control, over the value of the metric, preferably a reasonable idea of what would need to be done to drive it in the right direction.*

Prescriptive metrics define certain specific courses of action upon certain indications.[†] An example would be a compass showing a heading that is off course. It is prescriptive in that if you are to the left of the defined course, you need to turn right. If the oil pressure in your car drops to zero, the prescription is to stop the motor. If your security metric shows attackers rummaging through sensitive files, disconnect. Prescriptiveness is a very similar consideration to Actionability; the difference is that no decisions are required before acting on prescriptive metrics because the necessary response is self-evident or predetermined. Processes using prescriptive metrics experience less lag between measurement and reaction and may potentially be usable by juniors in the corporate hierarchy who would normally need to refer to their seniors for decisions or approval to act. This is analogous to the difference between real-time process control systems directly controlling plant and machinery, compared to higher-level SCADA systems that may require operator intervention when unusual situations occur.

Actionable also encompasses the idea of a metric being inherently stimulating and motivational: not only should the necessary action be reasonably obvious, but recipients of the metric should feel *compelled* to act.[‡]

* If the metric immediately responds to management's actions (much as the fuel gauge moves out of the red zone as soon as we refill), so much the better. Such positive feedback increases confidence in the metric and reduces hysteresis or lag. Such a factor might therefore be taken into account through either the Actionable or Timely criteria.

[†] There aren't enough letters in PRAGMATIC to cover all possible criteria or features of metrics that we might be concerned about. We mention a few others in this chapter. We inevitably had to make choices, based on our experience in the field, in developing a workable approach that is not overly complicated. You might feel that we have missed something important or included something irrelevant in the PRAGMATIC set, so go ahead and adapt the approach to suit your purposes. Though it works nicely for us as a mnemonic, we're not precious about it.

[‡] Almost any metric can be motivating if communicated appropriately (e.g., triggering the alarm when it crosses a certain threshold), but here we're talking about the intrinsic property of the metric itself rather than its presentation. For example, metrics relating to finances and legal/regulatory compliance tend to have a certain magical power over management that those relating to, say, technology seldom possess.

Tip: The PRAGMATIC scores provide a sound, rational basis underpinning what would otherwise be totally subjective opinions about good metrics. However, we acknowledge that the way metrics are scored against the criteria is inevitably influenced by the prejudices and biases of the people doing the scoring (see Appendix J). Three things can help here: (1) Do the scoring, or at least review and validate the scores, in teams involving representatives of the groups that will be receiving them: insist on consensus, and stop anyone (especially you!) dominating proceedings as dissenting voices often raise or hint at valid concerns; (2) keep brief notes regarding the thought processes and any factors that heavily influenced the scores: these factoids help make the PRAGMATIC scores themselves **Genuine** and will help immensely when the time comes to review and revisit the scores; and (3) practice.

6.3.4 G = Genuine

Genuine metrics provide unambiguous, straightforward, credible, and real information as opposed to spurious measurement artifacts or random noise. They are *reasonably* objective, such that someone else measuring the same situation would come up with the same, a very similar, or an equivalent result, rather than unduly subjective, in which case the result depends heavily on the prejudices, biases,* interests, and expertise of the person doing the measuring.

Some metrics gurus go so far as to insist that metrics *must* be absolutely objective, scientifically and mathematically sound. That might be fine if information security was a purely technical, scientific, or engineering domain (which arguably applies more to IT security than to the broader field of information security), but the reality is that some of the most important aspects fall in the realm of human behavior. Measuring security compliance in processes or staff motivations and awareness of security, for instance, inevitably involves a degree of subjectivity. The trick to developing good security metrics is to reduce the subjectivity where it is cost-effective to do so, but we are not in the business of conducting scientific research for the sake of it. It is unlikely many organizations would seriously consider engaging a team of independent trained psychologists or behavioral scientists to undertake an in-depth scientific study of an organization's security culture when a series of surveys or self-assessments and even anecdotal evidence will suffice to find out whether the culture is heading in the right direction.[†] With respect to security management, metrics that score below 100% on the **Genuine** criterion may be perfectly acceptable, especially if there is no practical, Cost-effective alternative way of measuring something important.

* See Appendix J.

† That suggests another moniker: G = Good enough!

Genuine also encapsulates the idea that a good metric should not be capable of being deliberately manipulated or falsified, which partly relates to the **Accurate** and **Independent** criteria. Metrics that draw on independently verifiable or auditable facts are more trustworthy than those that are opinion-based, but that's not always possible.

6.3.5 *M = Meaningful*

By this criterion we mean *Meaningful to the intended recipients, audiences, or users of the metrics*—those to whom the metrics are reported. Metrics must be readily interpreted by, and understood in the context of, the consumers. There is no point presenting low-level detailed operational metrics to senior managers, for instance.

Metrics are more than just a mechanism for presenting numeric information: good metrics are stimulating—they *encourage* the audience to *consider* and then *act appropriately* on the information. Metrics that just sit there passively in an appendix to a management report or tucked away in an obscure corner of a dashboard, day in, day out, are consuming and probably wasting a valuable resource. Management's attention span and ability to take in information is finite, so metrics are, in a sense, competing for head space. Later, in Chapter 11, we will discuss analytical techniques designed to get the most information and value out of our chosen metrics, but first let's think about the inherent qualities that make certain metrics more motivational and stimulating—intrinsically interesting in fact—than others.

There are several elements to this:

1. The metrics themselves may be relatively simple and straightforward, or they can be complex and unclear, bordering on impenetrable. Some are intuitively obvious and easily understood, whereas others may take some thought and interpretation, perhaps needing to be explained. Given the choice, metrics that are inherently **Meaningful** to the intended audience are more valuable than those that are confusing or obscure.
2. We've already mentioned that good metrics are **Actionable**: that's another PRAGMATIC factor, alongside **Relevance**, plus the value aspects that fall under the **Cost** criterion below. Together with **Meaning**, this all hints at the possibility of considering and perhaps actively addressing audience perceptions when finally discussing, presenting, and using your chosen security metrics.*
3. Communication/presentation methods affect the way information is understood. Metrics can resonate with the audience or turn them off: effective

* Chronic sufferers of SMD think about using marketing and promotional techniques to improve the perceptions of *their* security metrics, which is reasonable, up to a point. We risk losing the plot if our pet metrics aren't quite as shiny and diamond-encrusted in the eyes of our audience as they appear to us. Sometimes, we just have to let them go.

presentation techniques in the hands of passionate, talented presenters can make a huge difference, but it's easier for anyone to make an impact if the raw material is inherently exciting, motivational, and tells a good tale. While presentation is a distinct consideration that applies to any metric, if it would take a ton of work to put across a certain metric in a way that makes sense while another is blindingly obvious, sexy even, the choice (on the **Meaningful** criterion at least) is clear.

4. Metrics that relate directly or strongly to security outcomes tend to be more valuable than those that relate to the security processes and systems that will (eventually, we hope) generate desired outcomes. Security outcomes in this sense mostly involve reduced information security risks, meaning lower probabilities and/or adverse impacts of security incidents. However, some security controls, such as reviews and audits, and indeed security metrics, are valuable because they inspire confidence in the organization's information security arrangements. Greater management confidence is therefore a desirable outcome of worthwhile security metrics. Metrics that offer assurance tend to be **Meaningful**.
5. The maturity of the organization with respect to information security in general and security metrics in particular affects the ability of the recipients to understand and make use of different kinds of metrics. Put crudely, an organization that is just starting out on the security metrics road is likely to value relatively simple, straightforward metrics, whereas, months or years later, management will be more comfortable dealing with relatively complex issues, so more sophisticated and interesting (i.e., stimulating, thought-provoking, maybe even challenging) metrics may be welcome, albeit in addition to many of the original basic metrics that are still deemed **Relevant**, **Predictive**, **Genuine**, and, yes, **Meaningful**.

Tip: The context/situation and timing can be important. If the organization is currently going through its annual budgeting process, for instance, financial security metrics are likely to be well received if they catch the wave. Likewise, if management is conducting strategic planning or risk analysis, then strategic security and risk metrics will be appropriate. If management is in compliance mode, compliance-related metrics will be helpful—at this point, anyway.*

* Don't get carried away with this idea, however, because what was once the flavor of the month eventually ends up stuck to the bedpost... Still, it might be a good idea to schedule the presentation of annual financially based security metrics to coincide with the annual budgeting process and assurance metrics to coincide with the annual external audit.

Meaning is subtly different from **Relevance**. It is possible for metrics to be highly **Relevant** to security but utterly confusing to the audience. The frequency of security incidents, for example, may be easier to understand if reported in terms of the time since the previous incident rather than the number of incidents this year. Conversely, metrics that are **Meaningful** in the sense of being relatively straightforward and understandable (such as the number of viruses trapped this month) may actually be largely irrelevant to security.

Special care is needed with counterintuitive metrics. At a simplistic level, reports mixing metrics where high values are *good* with those where high values are *bad* can easily confuse the reader. Percentage values and numeric categories, for example, should ideally be calculated and presented consistently such that 0% or 1 always means terrible while 100% or 5 always means excellent.*

6.3.6 A = Accurate

Accuracy and precision of metrics can be more or less important, depending on the context. Most of the time, I'm not too worried if the fuel gauge in my car dips into the red as I know there's probably enough fuel left to get me to the next filling station, but for obvious reasons, a pilot would need much more **Accuracy** and precision about the remaining volume of fuel on the plane.

We may need to analyze the requirement in detail to determine how much **Accuracy** is required—or we may take a more PRAGMATIC approach. We are not looking for spurious precision (generally, one or two significant figures are sufficient for most security metrics), but we need to measure and report parameters with sufficient precision for recipients to plan appropriate, proportionate responses. Metrics that are relatively inaccurate may only indicate an issue if values are orders-of-magnitude apart from expectations, whereas more **Accurate** metrics may give an earlier warning of trouble ahead, hopefully in good time to avoid it.

Repeatability of a metric is related to its **Accuracy**. Repeatability is of particular concern in large or diverse organizations where a given metric may be measured by several different people, often in markedly different business contexts, and plainly, it is an issue for anything measured repeatedly over time. Random variability in the measurement process between measurements is likely to result in unpredictable discrepancies or inconsistencies in those measurements, reducing its **Accuracy** and precision. Conversely, a highly repeatable metric gives consistent results regardless of who makes the measurements and regardless of other factors that might introduce errors.

* Incident-related metrics can be a problem in this regard. Clearly, it would be fantastic if the number of security incidents was very low, but on the other hand, the proportion of security incidents reported should be very high. If we just report the number of incidents, that can tend to discourage incident reporting as much as it drives down incident occurrence. And, of course, impact must be considered as well as incidence. It's of little comfort to have very few incidents if the few that do occur are disastrous or catastrophic in magnitude.

Accurately measuring risk is a serious challenge because of its inherent nature: in contrast to information security incidents, such as typing errors, malware, or spam that occur frequently enough to be relatively easy to predict, infrequent incidents tend to be less predictable. Even objective or scientific risk assessment methods struggle to predict low-probability, high-impact incidents with sufficient accuracy or precision to guide risk management and security investment decisions. To a large extent, we are therefore forced to utilize risk indicators rather than risk measures as such.*

Another aspect related to Accuracy is the reliability or resilience of the metric. Murphy's law suggests that unreliable controls will fail at the worst possible moment—such as, for instance, an overloaded network intrusion detection system that fails to identify, report, or block a hacker or a worm penetrating the network under cover of the chaff thrown out. Unreliable metrics are similar. For obvious reasons, volatile indicators that suddenly go hard into the red without warning or constantly flicker between red and green are also not terribly useful as management tools.[†] Trends and averages, of course, level off such volatility over time but can also obscure or delay the revelation of genuine changes.[‡]

6.3.7 *T = Timely*

Timeliness in the PRAGMATIC context is mostly about minimizing the delay between collecting the data, analyzing them, presenting them, and facilitating corrective action. A metric that involves a company-wide survey of one in ten employees using in-depth interviews will take far longer to prepare, conduct, analyze, report, and interpret than, say, a focus group.

Timeliness has some bearing on the Predictive value of a metric, in that it's really not much help discovering today that we should have done something different last week or last month!

Timeliness is also relevant to a control principle known as hysteresis (see Figure 6.3). Hysteresis is normally considered in relation to physical controls, such as thermostats, but the principle applies just as well to information security.

* There's more to come in Chapter 9.

[†] Accuracy or, more correctly, precision is a serious limitation with so-called "traffic-light" or "heat-map" reports because there are generally only three possible values: red, amber, or green, whereas there are many situations in which something that is, say, toward the amber end of red implies something quite different from it being "so red it hurts my eyes!" Such distinctions may be addressed by footnotes and commentary in reports pointing out the true meaning, but the additional information detracts from the self-evident purpose of the simple color code. This is all a diversion, though, from the issue of selecting appropriate, worthwhile metrics. Even the best metrics can be ruined by crude or misleading presentation. The Accuracy criterion relates far more to the underlying precision of the measure than the way it is presented.

[‡] There's a tradeoff when configuring the number of measurements that are averaged for reporting purposes. Too few and the volatility makes interpretation difficult. Too many and important details are smoothed away. This is one of many issues to take into account in the analytical and presentational activities when developing security metrics.

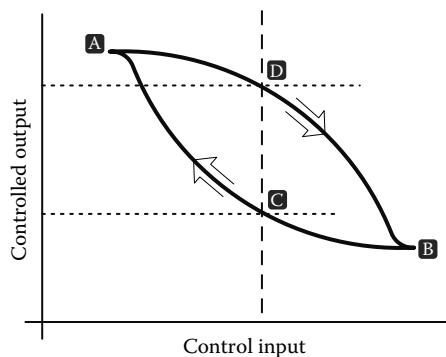


Figure 6.3 Hysteresis loop.

Starting at point A on the figure (the controlled output perhaps representing a certain level of information security risk), we apply some form of control, reducing the risk until we reach point B. Notice that, with respect to the origin, the upper A-B line is a convex curve: initially, we don't get much traction on the risk, but once the control becomes fully effective, the risk is reduced more rapidly until, finally, it levels off as we reach the limit of the control. Now, having reached stability at point B, assume we gradually relax the control and watch the risk level rise again, this time following the lower B-A line, a concave curve. Initially, the change in risk is hardly noticeable, but the control becomes less and less effective until eventually we find ourselves back where we started at point A. The Time lag between the control being applied and having its full effect opens up the gap between the lines, creating the hysteresis loop.* Note that at the control level, represented by the vertical dashed line, our risk level may be either at point C or point D shown by the horizontal dotted lines: in order to know which point we are at, we would either need to measure the actual risk (which is tricky) or know the history of how we reached that point (which curve are we on?).

The frequency with which a given metric can realistically be measured and reported is also of interest here. Organization-wide security surveys, for example, take Time and Cost money to conduct, limiting them usually to annual or sporadic events, whereas something such as cumulative financial losses due to security incidents this year can probably be calculated and reported on a monthly if not

* Limited hysteresis loops are *deliberately* designed into thermostats and similar physical and electronic controls (such as dusk lamps and motor controllers) in order to prevent the control and the controlled output both oscillating rapidly about the control point. If the control is too sloppy, however, and the loop is too large, the control and the controlled output both alternate lazily between the two stable states (creating a bistable, also known as a flip-flop). Arguably, the same considerations apply to information security control, including metrics, but this definitely qualifies as an advanced topic!

a continuous basis. If management reacts to the results of an annual survey, they probably won't know for sure whether they have done the right thing or gone far enough until the following survey next year. If unacceptably mounting losses trigger an appropriate response, there should be more or less immediate feedback in terms of a sustained downturn in the accumulating financial losses.

Timeliness also has meaning in the sense of the period, timescale, or outlook: metrics supporting strategic decisions should confidently Predict further ahead (albeit at a broader level of abstraction) than those supporting operational decisions. This aspect is therefore context-dependent: the criterion needs to be interpreted in relation to the nature and purpose of the metric.*

6.3.8 I = Independent

This criterion is about the metric giving a truthful, honest, credible,[†] and, most of all, objective representation of the subject of measurement. It's also about it being resistant to manipulation by someone trying to game the measurement system. All in all, the Independence score reflects the trustworthiness and integrity of the metric.

If you measure the wrong things, you risk accidentally encouraging behaviors that are in fact counterproductive. Furthermore, it may be hard to stop and reverse such changes by the time you realize what is happening (Hauser and Katz 1998). For example, measuring and reporting on the proportion of systems fully security patched can result in a lot of work to patch the final tranche of systems (some of which may be offline, in store, offsite, or broken, and, hence, relatively low risk in fact) and may even result in some vulnerable systems being arbitrarily declared out of scope or unsuitable for patching *purely in order* to improve the numbers. A better metric in that case might be the half life, that is, the time taken to patch half of the vulnerable systems, which disregards the remainder on the assumption that you routinely patch the most critical systems first (which is an important point: such a metric only works well in relatively mature and stable security environments and would be unhelpful in more chaotic ones). If that metric is measured consistently, it provides an overall target for improvement and the means of demonstrating whether patching is actually improving while smoothing over the specific details of each patch implementation.

* We know we said this was a practical approach, but we didn't promise it would be easy.

† The credibility of a metric is tricky to assess and score because, like beauty, it lies in the eye of the beholder. It is a matter of perceived value, the believability and trustworthiness of the metric, the underlying measures and measurement processes, and the metrician, all from the perspective of the audience, the intended recipients or consumers of the metric. Credibility is a highly subjective factor but no less important because of that. If it were possible to measure the difference in perceptions between the information security professionals providing the information and their audience, both would perceive a good metric to be highly credible. It's fantastic if their perceptions coincide on the same metric!

Tip: Be careful what you wish for: simply measuring something inevitably focuses attention on it and probably diverts attention from other matters that aren't being measured. If you measure and report anything, people will naturally respond by making changes in order to "improve" those metrics, especially if they are incentivized and highly motivated to do so, but even without strong pressure, subtle changes usually occur. Whether or not those changes do actually improve information security depends crucially on the design of the metrics.

6.3.9 **C = Cost**

Metrics are never totally free. Even if the raw numbers are readily available (e.g., the number of virus incidents logged last quarter in the help desk's problem/request ticketing system), there are inevitably Costs incurred in analyzing, presenting, and using them. We therefore need to account for, or at least be conscious of, the Cost of collecting, analyzing, and using metrics.

We are concerned here with the net value rather than literally just the pure Cost. The most valuable metrics are highly cost-effective, that is, the business benefits they offer far outweigh the associated Costs.* Certain types of metrics (such as those based on large surveys) are relatively expensive to collect, but the benefits in terms of the measurement information may be substantial enough to more than offset the Cost, particularly if there are no viable, cheaper alternatives.

Something else to consider is the opportunity Cost of selecting one metric over another. Given limited resources and management appetite for metrics, there are going to be some tough decisions to make when selecting metrics. In choosing to report metric A, we are probably (whether implicitly or explicitly) accepting that we will not be reporting metrics B and C. Such decisions are especially important in strongly conservative and usually rather large bureaucratic organizations as opposed to those that are smaller and nimbler because it is harder to reverse decisions that turn out to be bad. There are ways of mitigating the risk and reducing the opportunity Cost, for example, by using prototyping approaches to compare the utility and value of proposed metrics and investing more into the analysis and justification stages before forcing the decision between them.

We might also take into account the Cost of measuring

- Too little (management by gut feeling and guesswork; the dangers of making decisions that, with the benefit of 20/20 hindsight, were clearly wrong)

* Unfortunately, the benefits are often even harder to calculate than the Costs. Ranking metrics in terms of their Costs (at least roughly determined) can help by focusing attention on the most Costly ones: there may be opportunities to suspend or drop some of them in order to reassess limited resources to other more cost-effective and, dare we suggest, more PRAGMATIC metrics.

Tip: It is easy to gloss over the financial side of metrics and measurement, but paying attention to this aspect will help get management on your side. You might like, for instance, to develop a spreadsheet in which you estimate and add up the predicted annual Costs associated with each of your candidate metrics, taking into account the entire lifecycle from gathering the raw data through to making management decisions and seeing the effects. You could estimate the value of such decisions on some sort of rational basis (e.g., cutting incident costs by 5%). Such a Cost–benefit analysis could even inform an investment proposal or business case for your chosen metrics. On a more basic level, management may simply appreciate knowing that you are consciously rejecting metrics that are considered not worth the effort.

- Too much (wasting resources and, more importantly, diverting management attention from the *things that truly matter*)
- The wrong things (focusing attention on irrelevancies, diverting attention from more important matters)
- Things wrongly (inaccurate, error-prone, misleading, misinterpreted, or fraudulently manipulated metrics)

Valuable metrics are also, on the whole, quite clear and concise, providing the bare minimum of data free of superfluous details and distractions. Sifting little snippets of information from huge data sets tends to increase the Costs incurred in amassing, analyzing, and making sense of the raw data. Asking management to mentally combine or contrast multiple metrics in order to extract useful meaning would tend to score below those metrics that stand alone, being self-contained and self-evident at a glance. Once again, don't get distracted by the presentation of metrics, which is a distinct issue from selecting them. Good metrics can be badly presented and vice versa.

6.4 Scoring Information Security Metrics against the PRAGMATIC Criteria

To demonstrate how the PRAGMATIC method is used, we'll now work through the process of scoring a single metric, step-by-step, using a hypothetical but realistic metrics development scenario for illustration.*

* This is another sing-along audience-participation section (“experiential learning” the educationalists call it). Work it through with us. Treat this as a training flight, if you will, with us at the controls while you settle in and get familiar with the method.

Step 1 Determine the Measurement Objective/s

First, we need to figure out what we hope to achieve with our metric/s.* Consider the following situation. An important but almost universally neglected aspect of effective information security management is the organization's perception of the information security department. If, as is often the way, the department or function is perceived as something of an impediment to business activities, the bane of end user's existence, and the arch enemy of IT, it is unlikely to be entirely successful. If it appears that information security's knee-jerk response to virtually every request is "no," whether or not this is literally true, is it any surprise that the rest of the business will only approach security as a last resort?

To their detriment and peril, few information security managers make the effort to determine just how senior management, business owners, and end-users perceive them personally plus their teams. It is critical to understand that these folks constitute, in essence, the customers for information security; therefore, building more effective customer relationships is almost certainly worth the investment. Discovering and understanding customer perceptions provide an opportunity to do something to change them, which is where metrics come into play.

Our objective then is to measure the perceptions of customers of the information security department regarding its effectiveness and efficiency in such a way that the information security manager[†] can proactively manage and improve them and so make the department more successful.

Step 2 Specify the Metric/s[‡]

We'd like to know how well respected the information security department is by its customers, perhaps relative to other departments/functions. We would also like to know whether customer perceptions are actually getting better or worse over time as this information will be crucial if we are to manage them systematically rather than relying purely on guesswork.

That is fine as an initial or outline specification, but we really ought to continue.

* We don't know for sure at this early stage whether we are developing one lone metric, a few metrics, or a whole extended family of metrics, complete with "uncles" that aren't genetically related. The tendency is to develop and adopt loads of variants, but that's how measurement systems get completely out of hand. A significant advantage of the PRAGMATIC approach is that we're able to let the creative process mushroom and create as many as we like on paper because we will soon score and rank them in order to select out the one—two at a push—that works best.

[†] Notice that we have implicitly defined the primary audience for the metric who would normally also *own* the metric.

[‡] In the goal-question-metric approach, this step involves deriving meaningful questions pertaining to the goals or objectives previously declared. If you'd appreciate more advice on using GQM in the context of security metrics, we recommend Herrmann (2007) and especially Hayden (2010).

Tip: It is tempting to skim quickly past the objectives and specifications (next step) and just get on with it, but hold your horses. We strongly suspect many of the crappy metrics we see in the wild are the result of well meaning but naïve people doing exactly that. Just remember: ‘Steady - Aim - Fire’ works best in that sequence. There’s not much point in getting all PRAGMATIC about your metrics if you don’t understand what they are meant to achieve.* Take your time. Consider your options. Picture yourself presenting and talking about the metric to a somewhat cynical audience. Brainstorm to come up with a nice mind-map diagram of goals and anti-goals if it helps you think through and clarify the objectives. Then get on with it.

* Software/system development projects *finally* seem to be getting the same message. Whether you choose the classic SDLC waterfall, formal methods, RAD, SCRUM, or some bizarre, off-the-wall, extreme programming approach, the end result would *invariably* have been better and arrived at sooner, with less angst, if only it had been better specified in the first place. Over-specified is an oxymoron.

Earlier (in Section 3.2), we mentioned the need to measure *the right things* and report them to *the right people in the right format at the right time*. That phrase suggests four key dimensions on which to specify our metric/s:

1. The right things to measure are the customer perceptions of the information security department. That begs obvious questions, such as “Who are the customers?” and “Perceptions about what?” We would need to clarify both aspects in order to be able to develop and implement the metric/s. The customers can probably be guessed at based on past experience or determined more accurately by information security people keeping a tally of who they interact with (whether in face-to-face meetings, emails, or reports). The perception aspect probably concerns the level of respect garnered by the department.
2. The right people to receive our metric/s are the information security manager, obviously...but hang on, there are others (more below).
3. Determining the right format will be enormously helpful when it comes to designing the report/s later on. Along with the analysis of our metric/s, it’s something we discuss further in Chapter 11. For now, suffice to say that we envisage a graphical display or printed graph showing the relative perception scores, probably distinguished by audience groups, over time. To create a meaningful timeline, we will need at least two, ideally three or more, sets of measurements at different points, so we will probably have to settle for a simple table at first if indeed we choose to report the initial round of measures at all.

4. At the right time is an interesting question in this case. We probably don't want to be surveying opinions too often as that will start to annoy people, thereby depressing the very opinions we are trying to measure. On the other hand, we need to be able to create a timeline. A reasonable compromise would involve surveying different individuals from our audience population every so often such that no individual is surveyed more than, say, once a year.

Who exactly *are* the customers for information security management? There are many in fact. Here are the more obvious candidates:

- Colleagues, meaning employees who solicit or expect the function's help on information security matters. In stark contrast to the "no" department, a popular, well-respected, and effective information security management function gets consulted frequently on all manner of security, risk, and control-related matters, especially the IT security aspects. There is at least as much information pull as push. Truly appreciating that work colleagues are valued customers with genuine needs rather than just being annoying distractions goes a long way toward turning the "no" department into the "yes, but" department, and from there it's but a short hop to becoming the "yes" department.
- Management is a conveniently deep bucket into which we can throw junior, middle, and senior managers who, in addition to raising security, risk, and control issues, have governance concerns that often intersect the function's remittance and expertise. Managers make powerful allies and dangerous adversaries because of the power they wield within the organization. Keeping management sweet should figure high up on the information security manager or CISO's to-do list. After all, they *are* running the business.
- Information asset owners (IAOs) are worth highlighting as a key group of customers because they are special, in the everyday meaning of that word (nothing to do with special needs or the short school bus!). Assuming that management holds IAOs *personally accountable* for protecting the information assets that they "own" and provided they take their accountability seriously, they generally need to work quite closely with information security management to determine, specify, and, ultimately, fulfill the organization's requirements for securing their assets. IAOs are usually managers, often quite senior managers; hence, this group intersects the previous one, but because of the accountability, their interest in information security is more personal and real. If information security management succeeds in making IAOs feel they are special, there are significant benefits in terms of securing valuable business assets and making friends in high places. Ignore or upset IAOs at your peril!
- Auditors, particularly IT and ISMS auditors, are customers in that they often expect information security management to offer both information and assurance concerning the state of the security controls protecting information assets. It's generally a *bad idea* to ignore or upset the auditors, too.

Tip: Start with one of the example metrics specification forms that looks about right, and let it evolve until you are comfortable with it. You will soon get a feel for which items of information about metrics are most useful, which are tedious and unnecessary, and what level of detail is appropriate for your purposes. Don't forget to include the PRAGMATIC scores as you may want to review/update them later in the light of experience.*

* "Review them later" suggests a periodic process to go through all your security metrics, making sure they are, in fact, earning their keep and looking for improvement opportunities. It's one of the management activities suggested for the *information security measurement system* discussed in Chapter 8.

Other customers of the function include professional contacts and peers from the industry (meaning both the information security industry and the organization's industry or market segment) and, sometimes, the organization's suppliers, business partners, and customers—potentially even society at large.

We could leave it at that or set aside yet more time to clarify and elaborate on the specifications in as much detail as we see fit. A common approach typified by SP 800-55 (NIST 2008), the CIS Security Metrics (CIS 2010), and ISO/IEC 27004 (ISO/IEC 27004:2009) is to complete a standardized metric specification form of some description, filling in all the boxes for every metric. Of course, first you need to have prepared your template metrics specification form...

Step 3 Design the Metric/s

There is more to this metric than perhaps first meets the eye. Customer satisfaction is not just a feel-good factor. The effectiveness of the information security management function is evidently a concern if its customer-feedback scores are low. The perception of a lack of value from the function, for instance, is hardly likely to encourage other departments to seek out its advice and assistance on security matters. We sometimes joke about information security management being the “no” department, meaning a strident “No!” is the knee-jerk, instant, risk-averse answer to almost any security-related question. If so, is it any wonder, then, that colleagues

Tip: There are *loads* of ways of measuring customer satisfaction, but—relax—we're not going to bore you stiff now by laboriously describing them all here. If you genuinely want to know how to do it, either Google it or, better yet, go speak to a department or supplier who actually does it to learn the tricks of the trade. As with so many other security metrics, gathering the information is the easy part. Analyzing and making sense of the feedback is harder, and acting on it is the really tough part.

100 ■ PRAGMATIC Security Metrics

fear the worst and avoid even asking the questions unless they essentially have no alternative?

It may seem obvious already that we are heading toward an opinion survey, but actually that is not a foregone conclusion. We might, for instance, use feedback forms to gather data about customer perceptions following their interactions with information security people. This is a commonplace approach in seminars and training classes.

Potentially, we might opt for 100% sampling (i.e., asking every customer for his or her opinions after every interaction or series of interactions), but that would definitely annoy those who interact frequently. We could also get fancy with statistical sampling techniques to determine exactly who we survey, or we could settle for a more pragmatic approach: let's aim to collect, say, five completed customer feedback forms per week, trying not to survey the same person more than once or twice a year. Thanks to a suggestion in a team meeting, we will give a token gift to everyone who completes a form—a toffee will do.

One issue to take into account with customer service-type opinion surveys is that it's best to survey people shortly after they have completed an interaction with the service provider. If you leave it more than a few days before asking, they simply won't remember, so the quality of the data suffers. It's no big deal for customers who interact frequently with information security management, but for those who you only see once in a blue moon, you may need to trigger the survey process manually.

As to the actual survey, we could leave it completely open by asking customers what they thought of the interactions (which might generate a few helpful and detailed responses but mostly would solicit a bland and not-exactly-insightful "Oh, OK, I guess!"), or we could try a more structured approach by composing a standard survey form asking questions about perceptions such as the following:

- Would you say the information security person or people you dealt with were competent?
- Were you treated well, with respect?
- Was the interaction efficient?
- Did you get whatever you needed from information security?

Likert items* could be used to gain more meaningful and granular data from recipients beyond simple yes/no answers, perhaps something along these lines:

①	②	③	④	⑤
Not at all	Slightly	Possibly	Somewhat	Absolutely

* See Section 11.1.5. Obscure or confusing words such as "somewhat" are poor choices for a Likert item.

For even more granularity, you might use a percentage or sliding scale with scoring markers or examples (elaborating on those five points just listed) indicating particular points on the scale.*

Step 4 Rate and Score the Metric/s Using the PRAGMATIC Criteria

So how are we doing? How well does our candidate metric rate against the PRAGMATIC criteria? It's crunch time. The most straightforward technique here is to work systematically through PRAGMATIC letter-by-letter[†] using the all-important rating guide in Appendix B and taking good notes as you go:

- **Predictive:** this metric is predictive in terms of what needs to be done by the information security department to develop better customer relations in the future. However, the cause-and-effect linkage is not absolutely perfect, and even outstandingly brilliant customer perceptions would not prevent information security incidents, meaning it is not a strong predictor of the overall state of information security. The metric therefore falls *well* short of the 100% rating on this criterion. We'll give it 60% in the scoring table (see table on page 104).
- **Relevant:** for the information security manager who is the primary customer, the metric provides relevant information for managing the department's relations with its customers, but again, that is not really a major part of information security overall. Good customer relations will make the department somewhat more effective—"somewhat" being the operative word. The rating is mediocre, say, 60%.
- **Actionable:** if the output value of this metric is low, clearly something needs to be done, but what exactly? It is impossible to tell from the metric alone. It *might* be possible to analyze the survey findings in greater detail, for example, to determine if there seems to be an issue with particular information security people or customers, but with just five surveys a week, the data will be very limited. Another low rating.
- **Genuine:** information obtained by customer feedback surveys of this nature is indicative but, depending on how they are handled, may be heavily influenced by the information security people themselves. Even the toffees we mentioned in step 3 will skew the results slightly because, although they are just small tokens of appreciation, offering them is a nice gesture. Whether that is deemed a worthwhile boost to the department's perceived value or a

* There are examples in Appendices D and H showing what we mean. By the way, Likert scales with an even number of options force people to come off the fence, whereas if you provide a middle option, it's the easy way out for respondents who can't make up their minds or can't be bothered to decide.

[†] This is where the slightly annoying PRAGMATIC mnemonic comes in handy! You don't need to stick slavishly to the sequence in reality, and it's perfectly OK to pencil in the ratings and then reconsider them later.

bias to the statistics is something worth considering in scoring the metric on the **Genuine** factor. Rating quite low.

- **Meaningful:** the trick here is to picture the metric *from the perspective of the intended audience* as you consider the score. It's easy for this particular metric if you *are* the information security manager but takes a bit more effort if you are developing metrics for others, especially an audience with which you aren't especially familiar. This metric is reasonably meaningful to the information security manager who, to be successful, must manage customer perceptions. To accomplish this, he must know what they are. It rates well.
- **Accurate:** small-scale surveys may not be statistically accurate, but great accuracy is not necessarily required in this case. We are more interested to see how the numbers track over time than in the absolute scores at some arbitrary point. Repeatability is actually what we are after rather than accuracy per se, but in the absence of a repeatability factor in the PRAGMATIC method, **Accuracy** is a sensible proxy. It certainly doesn't merit 100% because of lingering concerns about whether responses might be influenced by members of the information security department (see **Independence**), but it also doesn't score 0% because the survey responses do at least provide a factual basis. Let's settle on a middling rating, almost sitting on the fence on this one (51%).
- **Timely:** by the time the metric is available for reporting, the corresponding interactions have long since finished, so it is probably too late to do anything about them, but as a way of managing the department's customer perceptions for future interactions (which is the objective), the metric would be fine. With just five surveys per week on average, they could easily be analyzed and reported to the information security manager—and perhaps published on the department's intranet site—once a month. It rates highly.
- **Independence:** this is an issue because information security people might start persuading, even bribing, customers into giving them good scores. This actually happens in practice! This rating is rather low.
- **Cost:** the costs of analyzing the raw data for this metric are minor—maybe an hour a month for someone to gather up the forms and pop the numbers into a spreadsheet. Provided we only ask a few questions in the survey, the customers are not going to be significantly inconvenienced either. Good rating.

Finally, we calculate the overall PRAGMATIC score for the metric.* The simplest way is to calculate the mean (average) rating: add them up and then divide the

* You may feel the PRAGMATIC criteria are incomplete. If you are a highly paid consultant, you might choose to customize or elaborate on the method, for example, by weighting each of the criteria to generate a weighted average index, altering the criteria, adding criteria, or providing scoring norms additional to those given in Appendix A. But just be careful not to go too far, making the process unnecessarily complicated, expensive (at least in terms of your valuable time), and harder to explain to management. In fact, you might even drop some of the criteria to simplify the process still further—it's entirely up to you.

total by nine, the number of ratings, multiply by 100 to converting it to a percentage, and round it off to the nearest whole number for the table:

<i>Information Security Metric</i>	<i>PRAGMATIC Ratings (%)</i>								<i>Score</i>	
	<i>Predictive</i>	<i>Relevant</i>	<i>Actionable</i>	<i>Genuine</i>	<i>Meaningful</i>	<i>Accurate</i>	<i>Timely</i>	<i>Independent</i>		
Information Security Management customer satisfaction rating	60	60	40	35	85	51	85	15	80	57%

In practice, it might take us a couple of runs through step 4, possibly even revisiting the earlier steps, to converge on a score that we are happy with.* You will notice that, as it happens, none of the ratings we chose exactly correspond to the defined 0%/33%/66%/100% rating points shown on the table in Appendix B. We have interpolated, that is, made an assessment of each of the factors to assign ratings part way between the defined points that we are comfortable with.

Step 5 Compare the PRAGMATIC Score/s against Other Metrics[†]

We have discussed the process in relation to specifying, developing, and scoring a single metric, but you will have noticed that there were points along the way where we faced several options. Below are some examples:

- We could use additional survey questions or change the wording of the questions themselves.
- The survey could use Likert items or categories, percentage scales, free-format text responses, or perhaps some combination of these (see Section 11.1.5).
- We might gather customer perceptions using follow-up interviews, scored by the assessor instead of directly by the customers.

* If we were scoring several metrics, perhaps variants of the one described, we might need to adjust some of the ratings to reflect their relative merits on particular PRAGMATIC factors. Percentage scales are ideal for that as there are 101 different integer ratings (0% to 100% inclusive), far more than we could realistically distinguish by this approach. We could even go to halves or decimal fractions if our SMD kicks in, big time, but, honestly, it's not worth it.

[†] In due course, compare the customer satisfaction metric score against other example metrics described in Chapter 7 and listed in the prototype metrics catalog in Appendix F. Do you agree that, on the whole, the 101 metrics that score higher and figure above this one in the ranked list are better, more valuable, more worthwhile, more PRAGMATIC metrics? And that those 52 below it are generally worse in various respects? Does the 57% score we assigned seem about right? If so, great; you are rapidly approaching the point where you can fly the PRAGMATIC method solo.

Tip: Bear these steps in mind as you consider the example metrics in Chapter 7, and by all means, disagree with the ratings and, hence, the scores we have calculated. We don't claim our ratings are correct: some may be quite wrong in fact, particularly as your background experience, work situation, and, hence, mindset are different from ours in various respects. The point of the exercise is that it is an exercise for you as, indeed, it was for us!

- We could collect more or fewer surveys per week, maybe even survey *everyone* but only during one week a month.
- We could thank respondents with toffees, apples, or certificates of appreciation.

It must be obvious, now, why there is no shortage of candidate security metrics. In this one narrow area alone, we could easily generate dozens of minor variants and a few distinctly different metrics with a bit of lateral thinking! Nevertheless, we could create additional rows in our scoring table for each one (probably just the ones that clearly have merit, discarding the ones that are definitely nonstarters without even scoring them fully), rate them, and come up with a top scorer.

We could also look at ways to drive up the individual ratings for our metric/s, by which means we would be improving the metrics and increasing their value.

That's the beauty of being PRAGMATIC.

Step 6+ Select the Best Metric/s for Your Information Security Measurement System

We won't go through the remaining activities now as they will be explained in more depth later (Chapter 8) after we have led you through the scores we assigned for approximately 150 example metrics in the next chapter. Suffice to say that the PRAGMATIC method has let us score and compare a bunch of candidate information security metrics in a rational and reasonably repeatable and defensible manner.

6.5 Other Uses for PRAGMATIC Metametrics

Aside from using the PRAGMATIC method initially to select information security metrics when designing the measurement system, it is just as useful to reevaluate your information security metrics at any point.* We recommend periodically updating and leading management through the PRAGMATIC metametrics to check that the information security metrics in use do still support the information

* We view the measurement system as a very practical, *applied* management tool. The business and information security contexts are dynamic, so the system *must* be allowed to evolve, or it will gradually lose its cutting edge.

Tip: With that in mind, even if you don't yet have formal management approval to establish an *information security measurement system*, you don't have to just sit back and wait for it: start using the PRAGMATIC approach now, on the quiet! Practice scoring, assessing, and comparing metrics when you have the odd free moment. Chat about metrics scores with your colleagues. Your efforts will be rewarded with a better initial design for the system when (finally, fingers crossed) the time comes for management to give you the green light.

security management system and, where appropriate, make adjustments. It's not a bad idea for management to take a step back and review the entire *information security measurement system* formally at a strategic level at least once every year or two. In between, it may be worth mentioning the measurement system in periodic information security updates or reports to management that analyze and present security metrics—just a line or two about specific metrics, possibly with their PRAGMATIC scores, will remind management that they have options regarding the information provided.

The individual scores may well change in the light of experience, sometimes markedly. Re-ranking or prioritizing the current crop of metrics may open the door to retiring and replacing the lowest-scoring metrics with more promising and worthwhile alternatives. There's an important point here: any measurement system is bound to go through a maturation process. It will inevitably take time to stabilize or settle down after being established.* Subsequent changes to the system should be controlled and managed just like other organizational and system changes. Metametrics give management the handle they need to make sure the measurement system is changed appropriately.

6.6 Classifying Information Security Metrics

In order to help management make sense of the vast range of possibilities when specifying and designing information security metrics or when reviewing/assessing candidate or current metrics, it helps to classify[†] (i.e., differentiate and categorize)

* That's why we recommend pilot studies or trials as a way to work through any teething troubles and finalize the initial design of your measurement system—the same process used by good software development projects in fact.

† Although “classification” as we mean it here is nothing to do with the classification of information in government and military circles, that does suggest yet another way to divide up metrics according to whether they relate to compliance obligations and for other externally imposed reasons or are purely for internal use.

the metrics in various ways. Classification of metrics into certain categories or groupings* makes it easier to pick out candidate metrics that might be of use in measuring a given topic of interest (such as privacy-related metrics) or might provide a certain type or stratum of information (such as high-level “helicopter view” strategic metrics for senior managers, or more detailed operational metrics for security analysts and technicians). Classification also encourages the development of a balanced suite of metrics, assuming that all classes are equally desirable.[†]

It is unrealistic to expect business types to beat down the security manager’s door with requests for specific metrics or to even know what can be measured or why it might be important.

With a moment’s thought, it should be obvious that there are many different ways to categorize or classify metrics. Let’s pick out a few to get you thinking.

6.6.1 Strategic/Managerial/Operational (SMO) Metrics Classification

Information security metrics typically support three distinct types of corporate decisions made, usually, at three different levels of the corporate hierarchy. The differences are very important to this book if not immediately obvious. Each of these levels needs a quite different type of metric to fulfill its function.

1. *Strategic metrics*: in loose terms, strategy is about seeing the bigger picture and determining in broad-brush terms where the corporation needs to be. More formal definitions of what constitutes strategy vary along with appreciation of their value. The original military definition is still the best in terms of clarity: strategy is simply *the plan to achieve one or more objectives*. Of course, this presumes that there are clear objectives, which, for information security at least, is not necessarily the case. Strategic objectives are navigational in the sense of formulating, envisaging, defining, or describing some grand destination for the organization. Strategic security metrics are primarily intended for and valued by senior management, typically covering major governance, risk, and control issues, and providing information to guide strategic corporate decisions. Crudely speaking, these are the long-timescale, broadly scoped, helicopter-view metrics, but there are subtleties to strategy development that sometimes require more detailed information in specific areas.

* Classification is essentially a crude form of measure. Rather than saying something is, say, 90% OK, we stick it in the green category. If it is 40% OK, it might still be green, but it is probably amber. Strictly speaking, there is no amber end of green as that would imply additional classes. Oops, my SMD just flared up again.

[†] A literal balance, equilibrium, or equality between the classes may not be appropriate in fact, but a complete lack or a perceived deficiency in any one class *may* be worth addressing.

Tip: Strategic information security metrics are *indisputably* linked to business or organizational goals. Any metric that does not have a direct, obvious relationship to one or more business goals is unlikely to qualify as a strategic metric. Making that relationship *explicit* gives true strategic security metrics superpowers because any excuses or counterarguments to justify underperformance infer the challenger's lack of support for business goals, which is a career-limiting move.

2. *Management/tactical metrics:* once the strategic objectives are clear, management's primary function is to devise the most efficient route to get there. Management involves putting the strategy into action, in a sense, steering, accelerating, and braking during the trip. The manager must figure out the route and the heading to the destination, taking advantage of viable shortcuts while avoiding obstacles. The manager doesn't need to know the nitty-gritty operational details; he or she only needs to know that the engine and the flight controls are operating within their normal range. In the context of information security, management metrics typically provide information to assist with the management and direction of the information security management function on a month-by-month basis.
3. *Operational metrics:* operational activities concern the mechanisms under the hood. Operations people must keep the wheels turning and the motor running. To do this, they need operational metrics indicating how well the machinery is operating and pointing out any fault or overload conditions on a day-by-day basis.

In the information security context, a metric on server patching, for example, is quite clearly an operational matter. Server patching, *per se*, is unlikely to be of any concern or make much sense to the CEO or board of directors: patching servers is hardly a strategic corporate objective. By the same token, strategic metrics are likely to seem rather vague and irrelevant to operations people. Managers have some interest in both strategic and operational metrics. IT management may need to know about server patching, not so much the patch status of any individual system but perhaps a summary metric, such as the proportion of critical servers that have been fully patched or the amount of resources and time needed to complete a round of patching.

As well as using the ISO/IEC 27002 structure, the example metrics in the next chapter are also classified (but not sorted) by SMO to illustrate the approach. If you are seeking inspiration on security metrics likely to be of interest to senior management, for instance, you can easily sort or filter the metrics catalog (Appendix F) by the SMO column with a click or two in the corresponding spreadsheet to pick out the S-level metrics.

Tip: Although we haven't classified the example metrics by all the other criteria discussed below, it's something you might like to do if (when) you develop your own security metrics catalog.

6.6.2 Risk/Control Metrics Classification

Because risks and controls are central to information security, many of the measures in this field naturally concern risks or controls. Measures of information security risks are intended to tell us what we are up against and help us focus on the risks that really matter to the organization. Some measures of information security controls tell us how well we are addressing certain risks and point out areas of strength and weakness in how we tackle the issues. In general, therefore, metrics relating to risks are more valuable to business managers, whereas measures relating to controls are of more value to security practitioners for operational reasons. Information security control-related metrics can be further classified in essentially the same way the controls can be classified, for example, by confidentiality, integrity, or availability (CIA) or preventive, detective, or corrective (PDC).

6.6.3 Input–Process–Output (Outcome) Metrics Classification

Generally speaking, we (or rather management) are most concerned with security and risk outcomes, in other words, the results of information security and risk management activities. Ideally, we want to know that our information security arrangements adequately address the risks, meaning the residual security risks are negligible or at least acceptable. Hence, in theory, it would be great if we could measure security outcomes directly. However, it is often impossible to do so in practice until after the fact, forcing us to measure the processes we believe will create the desired end results or even the inputs to those processes. The further upstream in the process timeline we move, the weaker the link to defined outcomes becomes, but still it may be better to measure inputs than to have no measures at all of important security processes. Obviously, the greater the demonstrated correlation between particular inputs or processes and specific outcomes, the more useful this approach becomes.

Take security patching for example: we can measure the inputs to the process, such as the timeliness of availability of security patches for known vulnerabilities, the process for assessing and applying relevant security patches, and we can measure the output of the process in terms of patches being applied to all relevant systems. However, we can only estimate the desired security outcome, which is that our systems are no longer vulnerable to exploits. The input, process, and output measures reduce our level of uncertainty and are important criteria for assessing and

managing the efficiency of the patching processes (e.g., the allocation of resources to patching activities).

There is, of course, a strong correlation between the patching process and the desired outcome, so in this case, the input, process, and output measures are a reasonably good guide to the outcome. However, in other circumstances, the correlation is not necessarily so strong. For instance, there are many different drivers determining the overall level of information security risk: we may have a handle on some of them, but we cannot control or measure them all. We can generally only influence rather than control security threats: we can guesstimate the threat levels, but we do not know all the capabilities and intentions of our adversaries, and there is a distinct possibility that we face as yet unrecognized threats that will only become apparent after they manifest themselves and cause an incident.

There are two types of process metrics: performance metrics, which have a predictive character, indicating the extent to which the process is performing in terms of activities, and outcome metrics, which indicate the extent to which the process really has achieved its goals and purpose.

COBIT 5 Exposure Draft

6.6.4 Effectiveness and Efficiency Metrics Classification

Metrics vary in terms of both their effectiveness (the extent to which they provide the information needed to support management decisions) and their efficiency (e.g., the cost of gathering, analyzing, presenting, and making sense of them). Given the choice, we would naturally choose highly effective and efficient metrics, but these are orthogonal (independently variable) criteria: unfortunately, some highly effective metrics are rather costly, complex, or difficult to understand, and many low-cost metrics provide information of low intrinsic value to management.

6.6.5 Maturity Metrics Classification

In our journey toward the best information security management practices, most of us naturally start out with relatively simple or naïve metrics, perhaps incorporating a smattering of commonplace metrics culled from the information security textbooks and blogosphere. Management finds such basic metrics easy to understand, and they tend to be cheap to produce, so they undoubtedly have their place. Unfortunately, the practical limitations of such metrics soon become apparent as the organization's approach matures. Issues such as focusing management attention on the wrong things, providing incomplete or misleading information, and forcing managers to manage through the rearview mirror lead us to search for more advanced or sophisticated metrics. This can work well, but there is definitely a risk

Tip: It is not necessarily appropriate to develop and implement a comprehensive, cutting-edge, highly advanced *information security measurement system* immediately, especially from a near-zero base. In fact, there is a distinct possibility it will crash and burn as a result of being far too ambitious for the organization. Don't forget that the recipients of security metrics also need time to come to terms with them and adapt their thinking processes to make use of them. Don't overload management and risk burning them out: you need them as much as they need you! It is much better to start out on a more realistic scale and let the system evolve naturally, working with management, discreetly using metameetrics to nudge it gently along in the right direction. You'll get there in the end.

of going too far too soon—for instance, developing clever security metrics that simply confuse or mislead the very people they are meant to help or incorporating so many metrics that they lose their impact and value.

6.6.6 Directness Metrics Classification

Some metrics relate directly to the subject of measurement with a causative perhaps even a direct physical relationship (e.g., the temperature and humidity of the computer suite), while others are more indirect and interpretive (e.g., the quality of the IT security architecture). We tend to refer to the latter as indicators because they indicate things of interest or concern in a broad and rather indistinct or imprecise manner compared to direct measures. You could equally try to distinguish objective from subjective metrics, although you will soon discover that this often involves shades of gray, arbitrary judgment rather than matter-of-fact, black-or-white distinctions.*

6.6.7 Robustness Metrics Classification

At some point, management may determine that the existing security metrics are simply not robust enough. If we are lucky, they will attempt to clarify what they mean by “robust.” More likely someone will utter an indistinct definition or offer a few rather vague requirements and expect you to come up with more robust metrics. It could equally be a call for greater precision or something more scientific, perhaps. One month, hard metrics might be in vogue, possibly as a result of something someone has spotted in an in-flight magazine or a chance comment

* Note that the SABSA metrics in Appendix E are classified as hard or soft. We are not entirely sure how.

from a colleague. Next month, the goal posts might shift toward soft measures or something else, and so the game continues.

As an information security manager faced with this kind of hand-waving and vacillation, you have to decide whether to push back, insisting on greater clarity from management, or simply to go with the flow, doing your best to interpret and satisfy what are often ill-defined if not ill-considered demands but which might genuinely reflect changing management needs, not just tastes.

We can't resolve such an awkward situation for you, unfortunately, but we can suggest some approaches that you might find helpful:

- Explain that you are struggling to understand their concerns with the current metrics or the pressure for something different. Ask for examples to illustrate, possibly a favorite metric from a field other than information security.
- Take a stab at classifying/grouping or rating/ranking a selection of potential security metrics according to your understanding of the requirements, and then get management to confirm whether you are on the right track. Try to establish which metrics are the closest to, and furthest away from, what they expect. Lather, rinse, repeat.
- Ask several managers for their opinions, attempting to identify and draw out common themes. If there are distinct camps with competing demands, point this out, and let management decide.
- Present sample metrics and ask management to reject the metrics that are the worst, developing a short list suitable for a trial or pilot study and, in time, a final selection.
- Distinguish the inherent qualities of the metrics from other potentially manageable factors, such as the way they are analyzed and presented. Would it help, for instance, if a certain metric was reported more or less frequently? If that makes a difference, the metric itself may not be so bad after all.
- Look for complementary or mutually supportive metrics. If the lack of robustness threatens to discount an otherwise valuable metric, would it help to provide another supplementary metric to compensate for the perceived weakness?
- Take a break. Come back to the issue later when the dust has settled and everyone has had a chance to think more clearly. Sometimes all it takes is patience!

6.6.8 Readiness Metrics Classification

This classification approach has limited applicability in the commercial world but may warrant some consideration. The following description is quoted from *Information Security Management Metrics* (Brotby 2009a):

Operational readiness metrics. This concept was drawn from the traditional military readiness measures of combat readiness. The IA posture of an organization can be measured by how well its units (systems, departments) and individuals are prepared to perform their assigned tasks of operating the system in a proper manner. Readiness measures are internally self-assessed or externally assessed by third party. An example of the IA readiness metric exists in a current Joint Chief of Staff Instruction (CJCSI) as a self-assessment checklist of IA related capabilities (e.g. “if adequate architecture for securing systems and networks is in place”). Operational readiness metrics can be further classified as management readiness related and/or technical readiness related.

Management readiness metrics measure management’s support of information security processes in the organization—for example, commitment, personnel and resource management, and risk assessment of intellectual property. These metrics are mostly static, i.e., these are questionnaire-based assessments and are generated by reviews of organizational policy and procedures with respect to the operations by interviewing management. An example is the frequency of regular audit trail reviews or operational procedure drills.

Technical readiness metrics measure the readiness state of technical support that affects the organization’s ability to provide information assurance while performing operational missions. They can be static or dynamic. Risk assessment and vulnerability analysis are examples of static technical readiness measurements. Information Assurance Vulnerability Alerts (IAVA) by Defense Information System Agency (DISA) require organizations to use IA metrics to remediate known vulnerabilities of the technical resources, keep track of remediated systems and report compliance status. Dynamic technical readiness assessments are more of a “live-play” exercise that simulates adversarial scenarios. Red team threat based efforts apply a simulated task force to expose IA vulnerabilities, as a method to assess the readiness of DOD components. A specific example of this type would be the Information Design Assurance Red Team (IDART) methodology used by Sandia National Laboratories which results in metrics such as attack percent completed, attack probability of success, and time/cost/skill in attacks.

6.6.9 Policy/Practice Metrics Classification

Information security requirements and obligations are defined and imposed in many different ways, but there is always a tension between the security rules that should be followed and what actually takes place in practice. *Both aspects are worth measuring.* Deficiencies in the rules (including gaps and conflicts) are only partly

covered by expecting employees to apply their discretion and do the right thing. Compliance failures can indicate someone's willful and flagrant disregard for the rules (perhaps malicious), a simple lack of knowledge, understanding or appreciation of them, carelessness and accidents, or something else entirely (perhaps even situations in which the rules genuinely do not apply). In any event, the metrics can provide information that management will find useful to improve information security.

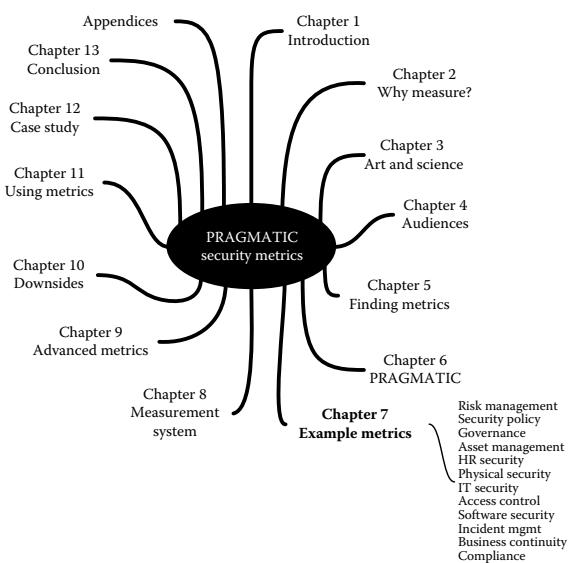
6.7 Summary

This chapter introduced the concept of metametrics, and then went on to demonstrate it in the form of nine PRAGMATIC criteria (**P**redictability, **R**elevance, **A**ctionability, **G**enuineness, **M**eaning, **A**ccuracy, **T**imeliness, **I**ndependence, and **C**ost). We described how to go about rating and scoring security metrics using the PRAGMATIC criteria, working step by step through the process for a single metric. The chapter concluded by pointing out the many different ways in which metrics can be classified or grouped.

Free ebooks ==> www.ebook777.com

Chapter 7

150+ Example Security Metrics



Mr. Jaggers suddenly became most irate. “Now, I warned you before,” said he, throwing his forefinger at the terrified client, “that if you ever presumed to talk in that way here, I’d make an example of you. You infernal scoundrel, how dare you tell me that?”

Charles Dickens, *Great Expectations*

Tip: The point is not to derive exactly the same ratings and scores as we do but to try out the PRAGMATIC method and see how it works for you in your situation.

We move on now to demonstrate the PRAGMATIC method by using it to score a selection of candidate information security metrics. The approach we have taken in this chapter is to do the following:

- Identify approximately 150 information security metrics that might be under consideration to support a broad swathe of information security-related decisions*
- Group, classify, or structure the metrics to help us make sense of them
- Rate the metrics against the nine PRAGMATIC criteria (Appendix B) using the method described in Chapter 6, generating an overall PRAGMATIC score and a set of accompanying notes for each metric
- Discuss the metrics and their ratings, pointing out the factors or reasoning that led us to rate them thus against the PRAGMATIC criteria making up their scores

Just as with the security metrics themselves, the PRAGMATIC approach is context sensitive; in other words, the scoring criteria may be interpreted differently under various circumstances. For the purposes of the examples in this chapter, we have assumed the evaluation of potential information security metrics is taking place in the context of a generic midsized commercial organization that has a relatively immature information security management system (probably not certified compliant with ISO/IEC 27001, but perhaps working toward that goal). The scores will differ, perhaps materially, in other organizations and business contexts, including your own, so by all means, disagree with the ratings and scores we have determined as you consider the examples in relation to your own business and security circumstances.

To structure the discussion, we chose to group or categorize the example metrics in line with ISO/IEC 27002:2005 for two main reasons. First, the ISO27k standards are well respected and well known globally, so the structure should be at least broadly familiar to most readers. Second, while the categorization of some controls and metrics is somewhat arbitrary, the ISO27k standards are reasonably

* The list is *not* intended to be comprehensive, exhaustive, or definitive: these are merely example metrics, a way to illustrate PRAGMATIC scoring. The high-scoring example metrics may not be relevant or applicable to your circumstances and needs, and you will almost certainly need to adapt or adopt others. Some were chosen specifically for their very low PRAGMATIC scores in the hypothetical scenario but may score much better in your situation.

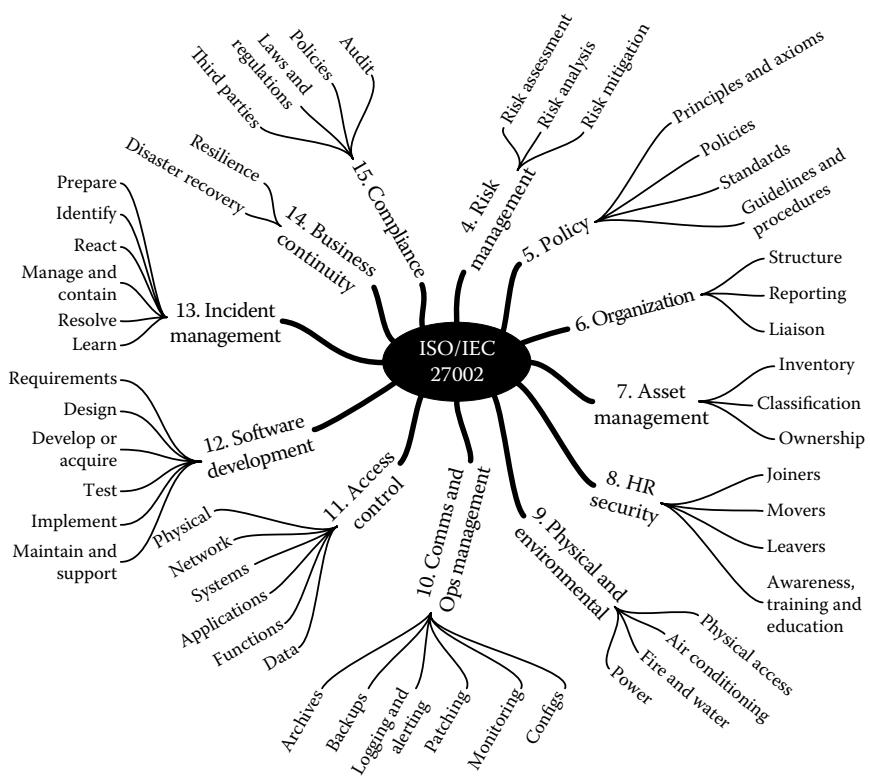


Figure 7.1 ISO/IEC 27002:2005 structure.

Tip: The PRAGMATIC scoring tables in this chapter are static snapshots from a spreadsheet we created, use, and maintain. The spreadsheet does the calculations for us and allows us to sort the metrics easily according to their PRAGMATIC scores or individual ratings. We can also weight the criteria if we wish to place more or less emphasis on certain ratings. Obviously, it's a lot easier to fiddle around with the numbers in a spreadsheet than to do the calculations and sorting manually. Although you can probably create your own spreadsheet easily enough from scratch, if you intend to work through these examples assigning your own ratings, or rating and scoring *your* information security metrics, you are very welcome to download ours as a starting point: visit www.SecurityMetametrics.com for details.

comprehensive and sound with few gaps, overlaps, duplicates, or conflicts. The ISO27k taxonomy suits our purposes. The mind map (Figure 7.1) gives an overview of the standard's structure.

7.1 Information Security Risk Management Example Metrics

Managing, meaning identifying and, especially, mitigating (reducing, ameliorating, avoiding, and occasionally eliminating) unacceptable information security risks, is essentially what the professional practice of information security is all about. Almost all information security metrics could therefore be included in this risk management category. However, we focus here on metrics measuring the *processes or outcomes* typically used to indicate, assess, and address information security risks.

Information security can be a business enabler. This goes beyond the obvious but rather negative target of security not getting in the way of business into the more positive realm of security facilitating reasonably safe exploitation of business opportunities. It is vaguely conceivable that an organization's strengths in information security might be the deciding factor to encourage management to launch a new product or attack a new market segment. More likely, however, is the situation that new business development proceeds with minimal concerns from management about security of the IT infrastructure and processes that underpin it, not understanding the full range of potential risks (ignorance is not an effective control measure!).

Risk is a tough area to measure and even harder to manage or control. We are particularly keen to identify key risk indicators (KRIs), that is, measures of significant change in information security risks, especially *leading* indicators that potentially enable us to identify and respond proactively to newly emerging or resurgent risks *before* a corresponding security incident occurs.

Tip: KRI *may* be a management buzzword, but it does serve as a convenient label for risk indicators or metrics that are important enough to justify management's attention. As you consider the summary table of possible information security risk management metrics opposite and read on to explore the example metrics and their scores in more detail, consider whether any of them would fit the bill as KRIs in your organization, bearing in mind that they typically serve primarily to initiate further investigation or analysis.

	<i>Information Security Risk Management Metric</i>	PRAGMATIC Ratings (%)										
		Score										
		Cost	Independent	Timely								
		Accurate	Meaningful	Genuine								
		Actionable	Strategic, Managerial or Operational	Relevant								
		Predictive	S M O	M								
		Strategic, Managerial or Operational	S M O	S M O								
4.1	Security risk management maturity	S M	92	98	68	78	90	83	89	84	92	86%
4.2	Number of high/medium/low risks currently untreated/unresolved	S M O	87	87	84	81	89	80	87	83	90	85%
4.3	Information security budget variance	M	70	90	85	77	80	77	80	90	95	83%
4.4	Process/system fragility or vulnerability	S M O	90	90	44	80	92	77	66	60	22	69%
4.5	Number of unpatched technical vulnerabilities	M O	80	64	80	70	80	75	25	85	52	68%
4.6	Information security risk scores	S M	72	60	55	70	71	40	60	60	50	60%
4.7	Total liability value of untreated/residual risks	S M	88	98	59	33	96	33	77	38	10	59%
4.8	Coupling index	S	68	85	50	60	72	47	35	61	42	58%
4.9	Changes in network probe levels	M O	50	80	10	68	66	85	50	70	40	58%
4.10	Organizational and technical homogeneity	M O	67	70	40	59	67	50	33	65	45	55%
4.11	Percentage of controls working as defined	M O	62	62	44	26	66	25	22	36	22	41%
4.12	Organization's insurance coverage versus annual premiums	S	64	46	5	25	20	16	10	82	94	40%
4.13	Number of attacks	M	13	9	1	2	12	1	4	1	7	6%

Example Security Metric 4.1

Security risk management maturity	P	R	A	G	M	A	T	I	C	Score
	92	98	68	78	90	83	89	84	92	86%

This is the first of several maturity metrics in our collection of more than 150 example metrics, one maturity metric for each of 12 metrics categories, in fact. Measuring the maturity of the organization's approach toward, in this case, the management of information security risks involves someone examining its risk management practices and comparing them to some sort of benchmark or standard. We envisage actually doing this in practice using a predefined suite of criteria denoting different points on a continuous scoring scale (see Appendix H).* The criteria describe information security practices considered typical or representative of organizations at various states of maturity. The scoring range extends from 100% (activities that substantially meet or exceed generally accepted good security practices, sometimes known as best practices) down to 0% (bad practices, perhaps even worst practices or abysmal practices).

There are at least six significant practical advantages to this type of scoring scheme or process using maturity scales with defined criteria:

1. The textual descriptions at each of the marker points provide a rational and reasonably objective way to assess and score each criterion while, at the same time, giving the metrician or assessor some latitude and discretion in assigning appropriate scores under the particular circumstances involved. With just a little training, any competent assessor should come up with similar or at least comparable scores in any given situation, despite the often subjective nature of the actual criteria.
2. The percentage scoring scale allows the metrician to interpolate between the indicated scoring points where appropriate. For example, something that doesn't quite satisfy the criteria for the 33% point might be assigned a score in the range of 20% to 32%, depending on just how close it gets.
3. In the way we routinely use and interpret the scales, 50% marks the distinction, boundary, or tipping point between slightly inadequate (49% or less) and barely adequate (51% or more) with the exact 50% midpoint reserved for those rare situations that are balanced precariously on the fence. Facing a security report containing a spectrum of metrics scores, a busy manager probably

* While we have provided a generic set of maturity scales in Appendix H, they are not meant to be definitive. Consider them a starting point for discussion and further development or customization. We have drawn on sources such as the ISO27k standards as well as our decades of experience to document the maturity scoring criteria, but your view of what constitutes bad through good security practices probably varies from ours—and that's cool. To be honest, if we started over today, we would probably come up with slightly different criteria because things are continually changing. In a year or two's time, some of our criteria may be even more markedly different.

ought to concentrate mostly on the values that are below 50% because they are, to varying extents, deemed inadequate. Used in this way, maturity scale metrics can substantially reduce the manager's burden through focusing on the issues that matter most. At the same time, values that are above 50% are, to varying extents again, good news, which is a rare and welcome commodity in the field of information security.

4. Percentages make readily understood scalar metrics, although it helps if they are used consistently, that is, 0% is always taken to mean an absolutely terrible score, and 100% implies perfection.
5. Scoring on maturity scales is a stimulating, thought-provoking process for the metrician. It takes a little more mental effort than simpler, more mechanistic scoring schemes, but that often leads to additional insight, much as the process of military planning might be said to be more valuable than the battle plans produced. The same point applies to the recipients of maturity scale metrics who can refer to and consider the scoring criteria (plus any notes or comments provided by the metrician) for clues about the maturity status.
6. Although it takes some investment up front to develop the initial set of maturity criteria, scoring against them is relatively quick (**Timely**) and cheap (**low Cost**) provided the metrician has gained a reasonable understanding of how the organization fares against the criteria, generally by gathering relevant evidence and talking to the people on the ground who know what's going on. Furthermore, the scoring process typically gets quicker each time the metrician uses the method as he or she gradually becomes more familiar with the criteria and perhaps refines them. The method works particularly well for repeated assessments, such as benchmarking/comparison of different departments, business units, or businesses, or for periodic reviews. Security consultants and auditors love it!

We prefer percentages over fractions and other forms of scalar, proportionate, or comparative numbers for scoring and ranking metrics because they are easy to interpret and compare. It is immediately obvious at a glance that a PRAGMATIC score of, say, 60% is lower than one of 70%, whereas it takes a little more mental effort to figure out that three-fifths is lower than seven-tenths. With 101 round-number values from 0% to 100%, percentages also provide more than enough precision for practically all security metrics purposes, and of course, we can use decimal fractions on the few occasions when even greater precision is appropriate. However, if you or your managers are uncomfortable with percentages, it's OK to revert to fractions or whatever, while even broad-brush categories, such as high/medium/low, are sometimes good enough.

Tip: The same pragmatic thinking applies to scalar, proportionate, or comparative security measurements (such as maturity scales) that are also usually best expressed as percentages.

Example Security Metric 4.2

Number of high/medium/low risks currently untreated/unresolved	P	R	A	G	M	A	T	I	C	Score
	87	87	84	81	89	80	87	83	90	85%

The number of information security risks that remain untreated or unresolved is an overall measure of the effectiveness of information security risk management, rather a measure of parts of it, because risks that have not been identified as a result of weaknesses in risk identification or analysis or that are not being properly tracked and managed would not figure in this metric.

Distinguishing significant risks (e.g., reporting the numbers of high, medium, and low risks, howsoever defined) is an obvious refinement for the metric because managers are probably not too concerned about low risks (they may simply be accepted), but the significant ones are clearly of concern.

Example Security Metric 4.3

Information security budget variance	P	R	A	G	M	A	T	I	C	Score
	70	90	85	77	80	77	80	90	95	83%

We interpret this metric to mean the variance between the budget for information security management this period compared to one or more prior periods. Significant changes (both cuts and boosts) to the budget are likely to affect the amount of security that can be achieved and may indicate changes in management's risk tolerance. The nature of those changes is not directly obvious from the metric in isolation, though; hence, the **Predictability** score takes a hit. The **Accuracy** and **Genuineness** of the metric depend partly on what the information security budget actually includes because some security controls are usually funded from distributed budgets and capital investments that fall outside the information security management department (e.g., the security parts of software developments are usually hidden in project budgets and are seldom identified separately).

Tip: {Metric 4.2} is a good example of a simple, straightforward measure that practically *begs* to be addressed by the intended recipients. It is implicit that untreated or unresolved risks, especially high risks, probably ought to be treated or resolved. The metric itself is highly **Actionable**, although what has to be done to treat or resolve the outstanding risks and whether that is cost-effective is another matter entirely. Tracking and reporting a metric like this over time should demonstrate whether management is getting on top of the organization's information security risks or is losing the battle. Either way, if framed appropriately and presented sensitively, the metric can be highly motivational.

Tip: For additional sophistication and bonus marks, contrast the results of theoretical vulnerability assessments on processes and systems against historical data regarding their actual real-world performance as an advanced information security risk management metric. Systems/processes that were designed to be highly reliable on paper but turn out to be somewhat fragile in reality probably deserve a closer look to figure out what might be causing the discrepancy.

Example Security Metric 4.4

Process/system fragility or vulnerability	P	R	A	G	M	A	T	I	C	Score
	90	90	44	80	92	77	66	60	22	69%

For this example metric, we envisage some sort of categorization or, possibly, an index ranking business processes or IT systems according to their fragility, vulnerability, or propensity to collapse in a heap at the slightest sign of trouble. The measurement process is likely to be quite subjective, although it may help to develop scoring criteria similar to the maturity metrics for higher scores on the Genuine, Accuracy, and Independent PRAGMATIC criteria.

Example Security Metric 4.5

Number of unpatched technical vulnerabilities	P	R	A	G	M	A	T	I	C	Score
	80	64	80	70	80	75	25	85	52	68%

This fairly easy-to-measure metric has value both in the absolute number of unpatched vulnerabilities (indicating the workload outstanding) and in the rate of change (a sudden increase could indicate a failure in the risk management processes—perhaps the workload is overwhelming).

Vulnerabilities are inherent security weaknesses in IT systems, business processes, etc., or (in some definitions) weak or missing information security controls. Vulnerability is just one component of risk alongside threat, exposure,* and impact, so knowledge of vulnerabilities is not enough, in itself, for management to decide whether and how urgently they need to be addressed. Vulnerabilities therefore need

* Vulnerabilities that are present are not necessarily *exposed* to the corresponding threats or impacts. For instance, a given vulnerability may be hidden in the depths of the organization under multiple layers of control; hence, the threat agents may be unable to reach and so exploit it. Although it is a weak control, security by obscurity may involve ensuring adversaries are unaware of exploitable vulnerabilities by keeping them hidden, that is, unexposed.

Tip: This metric could be adapted to consider vulnerabilities other than just software or technical vulnerabilities. Additional data on different types of vulnerability or weakness would turn this into a richer, more informative, and, we hope, more Relevant, Predictive, interesting, useful, and valuable metric for management. Going the extra mile to estimate and report the severity or gravity of the vulnerabilities (based on some combination of probability and impact) rather than just their number, the metric will gain real traction, albeit at still greater Cost and complexity.

to be checked to determine whether there are indeed corresponding threats, exposures, and impacts of concern to the organization.

The example metric disregards *unknown* and, hence, currently unpatchable vulnerabilities, plus nontechnical vulnerabilities, for example, physical vulnerabilities (such as locating a business in a seismically active region) and vulnerabilities in business processes and relationships (e.g., a critical dependence on the suppliers of vital information or IT services). It implies the use of vulnerability scanning software that identifies missing patches and, potentially, additional vulnerabilities in software systems. Software vulnerability assessment tools are not 100% accurate: most rely heavily on identifying and checking installed programs against signatures of known vulnerable versions. Time lags are therefore an issue because it takes time to identify and characterize a vulnerability, put the corresponding signature into the scanning tools, scan the systems, examine and assess the output, and finally react appropriately to the findings. That's why the Timeliness score is so low, and the Costs of performing all those steps are also taken into account. The metric can be expensive to measure, especially if, for instance, you use multiple scanning tools or use more advanced tools that test for additional holes but produce technical reports that can only be interpreted by geeks.

Example Security Metric 4.6

Information security risk scores	P	R	A	G	M	A	T	I	C	Score
	72	60	55	70	71	40	60	60	50	60%

Numerous frameworks, approaches, and methods exist for identifying and assessing information security risk.* The methods of decomposing and analyzing risks differ as does their granularity or depth of analysis, but overall, they are more

* For a handy list of standards, methods, and tools supporting information security risk analysis and management, see the ISO27k FAQ at www.iso27001security.com/html/faq.html#RAmethods.

Tip: The selection of risk methods should be primarily based on form, fit, and function. All the approaches have strongly subjective elements with Accuracy depending more on the assessor than the assessment per se. Consequently, there is always a significant amount of uncertainty that must be factored in, and the biases of the assessor must be considered and preferably compensated for (see Appendix J).

alike than different. There is no inherently superior, universally applicable solution (despite practitioners' and vendors' claims to the contrary!).

Most methods generate a simple numeric rating for identified risks. If one were to analyze an identical situation scientifically, comparing results obtained with a range of risk assessment tools, the risks themselves and the absolute risk scores would undoubtedly differ, but the relative levels or the rankings would probably be vaguely similar, slightly depressing the Accuracy score.* The better methods would be more consistent over repeated analyses, even if successive analyses were performed by different individuals. Luckily, all the methods generate useful information and insight in the course of the analysis as well as the final output.

Busy and/or naïve managers tend to appreciate the simplistic risk scores and the implied ranking of risks according to their significance (whatever that means!), whereas information security and risk management practitioners find more value in the analysis and the components of risk.

The **Costs and benefits** associated with the use of risk scores as security metrics reflect the depth of analysis performed: high-level or cut-down methods are quicker and cheaper but generate less valuable insight, and the risk ratings have wider margins for error. Nevertheless, they may be useful for an initial broad-brush sketch of the risk landscape. More in-depth, detailed analyses generate more specific, detailed answers and more precise risk ratings but typically cover narrower areas of scope and are more expensive in terms of the time and effort required. We don't know which type of process would be used in our hypothetical company, so we rate it at a neutral 50% on **Cost**.

Because *all* threats can never be known, nor can *all* vulnerabilities be found and *all* possible impacts be determined, no risk assessment methodology will provide ideal PRAGMATIC metrics. Accuracy and other **Genuineness** will always be left wanting. While this is not an argument against attempting to measure risk, it is essential to recognize that, at best, we can come up with probabilities with fairly

* We are not presently aware of any studies scientifically comparing methods for assessing and scoring information security risks specifically (financial risks are in a different league). For that matter, different approaches to scoring and ranking metrics would also be worth comparing on a scientific basis. Either aspect would make a fascinating topic for a masters or doctoral thesis!

low confidence and high margins for error.* What can be helpful is to determine the “tails” of probabilities, particularly the likely upper bounds of risk, on a reasonably rational basis. This is the essence of worst case scenario planning. Assessing inputs into the risk equations is where the calibration discussed in Appendix K can be useful in coming up with more Accurate results in terms of greater certainty or, more precisely, revealing the degree of uncertainty in the risk ratings.

An important consideration in any risk assessment/measuring activity is its credibility, especially to senior management. Security professionals are often tarred with the Chicken Little tag—“the sky is falling, the sky is falling,” and we’re doomed. There is a tendency to present management with the worst possible outcomes, regardless of how improbable they are, rather than the most likely ones. This has the unfortunate effect of causing our admonitions to be ignored or discounted.[†] Many of us have experienced the familiar response: “It hasn’t happened yet, and we’ll just deal with it if and when it ever does.” Limited credibility is reflected in the **Genuine** and **Independent** ratings.

There are many potential variants of this metric. For example, it may be worth checking whether business impact analysis (BIA, strictly speaking, an integral element of risk analysis and business continuity but often conducted separately) is being performed routinely and promptly by all software development and change projects: comparing dates and resource utilization on BIA reports against dates on the corresponding business cases, project plans, etc., specifically identifying any projects that either don’t appear to have any BIA planned or seem to have skipped or skimmed it, would be a metric to drive up the use and quality of BIAs.

At a higher level of abstraction, taking the view of security as a market differentiator suggests metrics such as the organization’s perceived information security risk/security status relative to its peers and competitors as determined by surveying the opinions of customers or other stakeholders.

Example Security Metric 4.7

Total liability value of untreated/residual risks	P	R	A	G	M	A	T	I	C	Score
	88	98	59	33	96	33	77	38	10	59%

* Business continuity management and the associated metrics are discussed in Section 7.11.

[†] Warnings of impending peril must be handled with care lest we’re merely to be considered hypochondriacs. The flip side is, of course, failing to warn of a risk that manifests, causing serious damage that can be even more career limiting! It helps to have some appreciation of and empathy with the audience, tailoring the presentation or report to achieve the most effective response. It is an area where corporate culture can play a significant role (see Section 7.5). If the culture is characterized by a high-flying, devil-may-care, pedal-to-the-metal sort of attitude, dire warnings in writing may be the only hope of getting a rational response to identified significant risks. If, on the other hand, the culture is more conservative, presentations should be more considered and well supported with evidence.

{Metric 4.7} attempts to put an overall dollar figure on the untreated or residual information security risks. It assumes that we can estimate liabilities, normally by calculating the product of impacts and probabilities for identified risk.* Both of those parameters can only be estimated and usually very approximately at that. The metric is therefore highly subjective and error-prone, which cuts into its Accuracy rating.

The skills and effort needed to calculate the liabilities (including inputs from many business managers as well as risk and financial specialists) make this a very Costly metric too, although if analyzing business risks and maintaining the risk inventory is accepted as an unavoidable cost of business, they may already be largely accounted for.[†] The Actionability rating is also low because it is unclear what management would be expected to do in response to the metric aside from perhaps adjusting the risk management budget.

On a more positive note, the liabilities represented by residual risks are certainly Relevant to information security and, in the form of large dollar figures, are likely to be highly Meaningful to management.

Example Security Metric 4.8

	P	R	A	G	M	A	T	I	C	Score
Coupling index	68	85	50	60	72	47	35	61	42	58%

{Metric 4.8} has nothing to do with sex but everything to do with relationships.

The rationale behind this metric is that knock-on impacts following incidents are more likely and tend to be more serious for IT systems, networks, business processes, and supply chains that are tightly coupled, linked together, or integrated than if they are loosely coupled or largely independent.

Contrast traditional mainframe financial systems against real-time ERP systems, for instance:[‡] if something causes a single mainframe batch to fail, it can generally be corrected and rerun without too much trouble, provided it still completes within the batch window. A similar failure on an ERP system can sequentially topple a whole series of highly interdependent operations, bringing the entire ERP and the associated business activities to a crashing halt—the domino effect.

* To complicate matters further, consider the possibility of significant incidents occurring completely out of the blue; in other words, the organization is blindsided by a risk that was never recognized as such, and hence, its magnitude was never determined. That's why it is vital to set some of the risk management budget aside for contingencies.

[†] Security metrics sometimes get a free ride on the back of other business activities. The incremental effort involved in adapting or exploiting existing business and financial metrics for security purposes can make them quite cost-effective with the added bonus of making security very much an integral part of the business, not an optional add-on.

[‡] We are not arguing in favor of one approach over the other: the architectures and business processes are simply different. The measure concerns the fragility arising from elements being tightly coupled or integrated together.

It would undoubtedly take time and effort to prepare and analyze a coupling index (e.g., to evaluate dependencies and links between systems, etc.) using techniques such as business and supply chain analysis, hence the poor **Cost** rating (it is not a very cost-effective metric). The **Timeliness** rating is also quite low for the same reason; plus, in practice, the true extent of coupling is often only appreciated during or after a disruptive incident by which time, of course, it is too late to do much about it. Provided useful information about the extent of coupling is available before the event, though, the metric is **Actionable** by, for example, improving business continuity management (particularly robustness and resilience) and, conceivably, adopting architectures that either attempt to decouple critical business systems, processes, supply chains, etc., or provide redundancies, although these actions are not easy and may not be feasible. This is the kind of metric that might be taken into account by senior executive managers when formulating overall business and information management strategies, including BCP; hence, it is categorized as a strategic metric. Middle or junior managers, architects, and operations people probably would not have the latitude to determine or alter the extent of coupling in any significant way other than advising and prompting their bosses to understand the risks and possible mitigation options.

Example Security Metric 4.9

Changes in network probe levels	P	R	A	G	M	A	T	I	C	Score
	50	80	10	68	66	85	50	70	40	58%

This is not a highly **Predictive** metric: network probes could be coming from competent hackers, script kiddies, or malware, and most are unlikely to be directed specifically at us or our systems. Phishing and other social engineering-type probes also tend to be blasted out indiscriminately via spam and Web sites. Identifying more dangerous probes that are either highly sophisticated or specifically targeted (e.g., spear phishing) is tricky (and hence **Costly**) at least in advance of the attacks they precede (so it is not **Timely** either) because they tend to be relatively low volume and stealthy.

How, or even whether, we should respond to an influx of probes is not at all obvious from the metric (e.g., we cannot necessarily isolate systems or networks that appear to be under attack because that reduces their availability, and, anyway, it may only delay rather than deter the attack), giving the very low **Actionability** rating. The metric should be **Meaningful** to a technical audience but would probably need to be explained to general managers, emphasizing once more the need to determine metrics audiences.

Example Security Metric 4.10

Organizational and technical homogeneity	P	R	A	G	M	A	T	I	C	Score
	67	70	40	59	67	50	33	65	45	55%

Tip: Keep an open mind when specifying and assessing metrics, and you might just find a metric that simply doesn't work out as originally envisaged turns out, with slight adjustments, to be ideal for a different purpose, perhaps months or years later. This implies not automatically deleting/discardng low-scoring metrics from your metrics catalog, within reason (get rid of metrics that are patently completely hopeless or that basically duplicate others: they are distracting and unhelpful, but do keep notes on any you retain).

Homogeneity (the extent to which the organization and its processes use or rely upon a limited number of technologies, suppliers, contracts, etc., also known as monoculture) increases exposure to aggregated risk: security risks that are acceptable in isolation become unacceptable when taken as a whole due to facing common threats. On the other hand, homogeneity means standardization, lower complexity, and economies of scale, which offer substantial business benefits.

Options for responding to the metric if it indicates too much or too little homogeneity* may include deliberately increasing or reducing heterogeneity, respectively or using compensatory controls, such as business continuity, slick network monitoring, network segmentation, etc.

The metric rates poorly on **Timeliness** and **Cost** because of the time and effort needed to gather and analyze the data with any kind of precision, although a quick-and-dirty assessment *might* be enough to get this issue raised and discussed at the top table, which (depending on the measurement objective) might be sufficient.

Example Security Metric 4.11

Percentage of controls working as defined	P	R	A	G	M	A	T	I	C	Score
	62	62	44	26	66	25	22	36	22	41%

Provided information security controls are being systematically tested to ensure that they satisfy defined control objectives or requirements, in theory, it shouldn't be too difficult to determine what proportion[†] of them fulfill the requirements.[‡] In practice, this metric would be **Costly**, slow, and difficult to measure on a broad basis. Because certain security controls may have to be tested for SOX compliance

* Too much or too little relative to what? We are hinting here at the definition of boundaries or limits on the values, a common approach with many metrics. We go into more depth on this aspect in Section 9.7.

[†] We prefer to represent proportions unambiguously as percentages. You might prefer to think in terms of fractions or pie charts. These are mere presentational details that don't affect the metric's inherent qualities being rated here.

[‡] This could equally have been classified as a compliance metric, a mere taxonomic detail but a reminder to check your metrics short list for unnecessary duplications.

reasons, however, the metric may have utility within the scope of the SOX-relevant systems and processes.

Example Security Metric 4.12

Organization's insurance coverage versus annual premiums	P	R	A	G	M	A	T	I	C	Score
	64	46	5	25	20	16	10	82	94	40%

If the organization spends \$50,000 a year to provide \$1 million of business interruption insurance coverage, the risk appetite has been partially quantified: management has evidently determined that risks that could conceivably result in \$1 million of business impact warrant an annual expenditure of \$50,000 on the control.

The metric may have specific applications, but the poor PRAGMATIC score means there are probably better alternatives.

Example Security Metric 4.13

	P	R	A	G	M	A	T	I	C	Score
Number of attacks	13	9	1	2	12	1	4	1	7	6%

“Attack” would have to be carefully defined in order to make this metric even remotely objective and repeatable, explaining most of the low ratings. As worded, it ignores the fact that attacks vary markedly in terms of the impacts caused, and information security incidents caused by accidents or by natural events, such as severe storms, are completely out of scope. The metric has a little **Predictive** value in the sense that a substantial upsurge in the number of (detected) attacks probably signals an increased level of threat and perhaps a greater probability of being compromised. A marked reduction in the number of (detected) attacks does not necessarily mean the threat has receded, however: it is just as likely that the detection rate has fallen, usually because the attacks have become more sophisticated and stealthy or the detective controls are failing (which could itself be a useful piece of information). Aside from knowing that we probably ought to be doing something about the upsurge, the metric leaves us completely in the dark about what to do. The 1% **Actionability** rating is on the generous side!

7.2 Information Security Policy Example Metrics

Policies are an important vehicle through which management formally lays out its intent and direction for information security activities. The process of considering, scoping, documenting, approving, issuing, and maintaining policies is arguably as important as the policies themselves in that it raises management’s awareness of the

<i>Information Security Policy Metric</i>	<i>Strategic, Managerial or Operational</i>	PRAGMATIC Ratings (%)							
		Score				Cost			
		Independent		Timely		Accurate		Meaningful	
		Genuine		Actionable		Relevant		Predictive	
		S		M		M		O	
		S	M	S	M	M	O	S	O
		75	90	80	90	88	95	80	90
		82	95	70	95	80	90	85	90
		92	90	88	91	91	95	84	82
5.1	Number of security policies, standards, procedures, and metrics with committed owners	87	90	95	92	92	77	92	90
5.2	Security policy management maturity	88	95	70	80	88	90	85	88
5.3	Traceability of policies, control objectives, standards, and procedures	89	88	90	91	87	65	84	85
5.4	Number of important operations with documented and tested security procedures	91	95	91	85	95	84	62	90
5.5	Comprehensiveness of security policy coverage	82	92	78	80	70	73	60	81
5.6	Policy coverage of frameworks, such as ISO/IEC 27002	75	90	69	85	76	72	65	85
5.7	Number or proportion of security policies addressing viable risks	73	91	73	83	77	70	61	78
5.8	Quality of security policies	80	85	40	66	72	75	80	80
5.9	Percentage of policy statements unambiguously linked to control objectives	91	64	60	85	65	45	75	75
5.10	Thud factor (policy verbosity/red tape index, waffle-o-meter)	82	80	60	70	45	35	86	84
5.11	Number of security policies whose review/re-approval is overdue	54	88	14	97	77	43	90	89
5.12	Flesch readability scores for information security policies, etc.	68	77	60	86	35	70	64	88
5.13	Number or proportion of security policies that are clear	75	70	68	41	96	50	56	90
5.14	Percentage of security policies that satisfy documentation standards	66	47	79	45	74	38	44	50
5.15	Number of security policies that are inconsistent with other policies or obligations	60	49	76	43	88	45	41	43

issues and forces them to think through and make themselves crystal clear about what they expect.

It may be difficult or impossible in some situations to discipline or fire employees unless they have contravened a stated requirement, such as a policy, while policies also drive awareness/training activities and are the basis for standards, procedures, and guidelines.*

A controls policy—a policy on controls—is a rare but valuable beast. The idea is to define how various controls should operate in various situations. For example, should controls fail open (insecure but not blocking the associated business activities, e.g., a firewall that passes traffic without deep inspection if it is overloaded) or closed/safe (secure but blocking, e.g., the overloaded firewall simply blocks further traffic)?† Should things be permitted unless specifically denied or denied unless specifically permitted? These are largely strategic or architectural issues that may be defined as overarching security principles or axioms, but they must be considered when designing controls and the associated metrics to ensure consistent design and implementation, that is, to avoid controls operating at cross purposes.

Example Security Metric 5.1

Number of security policies, standards, procedures, and metrics with committed owners	P	R	A	G	M	A	T	I	C	Score
	81	87	90	95	92	92	77	92	90	88%

Ownership, along with accountability and responsibility, are important yet (in our considered opinion) seriously undervalued concepts in information security. In the case of information security policies, procedures, and standards, clear ownership by suitable authority figures (generally senior managers) makes it far more likely that they will be championed, mandated, adopted, and maintained. In contrast, unowned policies, etc., simply don't have as much influence or impact and tend to end up lost and forlorn, languishing unloved and ignored in some corporate backwater.

By extension, the same applies to metrics. If they don't belong to anyone, nobody takes much notice or care over them.

Policies, standards, procedures, and—yes—metrics qualify as information assets; hence, they ought to have nominated information asset owners. Ownership is arguably best assigned to corporate roles rather than individual people to reduce the possibility of them being orphaned when people inevitably move on.

* It is a common misconception that guidelines are always entirely optional, a result largely of their name and informal writing style: in fact, they often offer guidance and advice relating to *mandatory* obligations defined in laws, regulations, or policies.

† The related issues of fail-safe controls and fail-safe metrics are covered in Chapter 9.

Tip: It is hard to do, but try to find business owners for as many security metrics as possible rather than having them *all* fall to the information security manager—even if this involves horse-trading, the information security manager accepting ownership of business/financial/other metrics relating to the information security management function. If you followed our earlier advice by clarifying the objectives and audiences for your metrics (Section 6.4), assigning ownership should be slightly easier.

Example Security Metric 5.2

Security policy management maturity	P	R	A	G	M	A	T	I	C	Score
	90	95	70	80	88	85	90	82	88	85%

As with the other maturity metric examples, we envisage using a scoring scale with predefined good practice criteria to measure security policy management in a reasonably scientific and repeatable manner (see Appendix H). Once again, the scoring process or the meaning of the final score may need to be explained to management, for instance, highlighting criteria against which the organization scored relatively strongly or weakly.*

Example Security Metric 5.3

Traceability of policies, control objectives, standards, and procedures	P	R	A	G	M	A	T	I	C	Score
	85	89	88	90	91	87	65	84	85	85%

{Metric 5.3} implies that there should be explicit linkages between all those elements.[†] It requires someone to examine the entire suite of materials, mapping out the relationships systematically to identify orphans and potential conflicts (e.g., if information security policies relating to personnel issues are owned jointly by both

* Assessing process maturity implies that the assessment criteria have been identified and preferably agreed upon: the very act of doing so could itself be taken a sign of maturity in the organization's approach in this area. This is a specific illustration of a general point: management's interest in metrics implies a certain level of maturity to the organization's information security program in the sense that metrics enable management control in a rational, systematic way.

[†] In our experience, ready traceability along with defined ownership/accountability for policies, etc., are good practices, indicative of relatively strong information security governance. This situation therefore exemplifies the value of taking a *systems* approach to the selection/design of information security metrics, selecting metrics that complement and support each other (e.g., metrics measuring both traceability and ownership/accountability of policies) rather than simply viewing and, in fact, scoring them in isolation. The systems aspect is explained further in the next chapter. By the way, shouldn't your *metrics* be traceable, too?

Tip: If you are taken aback at the effort involved in gathering and analyzing the data for this metric, start by examining those processes/systems with business continuity arrangements in place as these are evidently considered essential to and by the business.

information security and human resources, what happens if there are disagreements between these functions on the policy details when initially created or subsequently updated? Who has the authority to grant policy exemptions?). Dealing with the issues arising will be slow, giving the low Timeliness rating.

Example Security Metric 5.4

Number of important operations with documented and tested security procedures	P	R	A	G	M	A	T	I	C	Score
	95	96	91	85	95	84	62	90	60	84%

Well-written procedural documentation captures, codifies, and clarifies knowledge; provides step-by-step explicit instructions; references or incorporates mandatory requirements, obligations, and conditions; and incorporates manual controls. Procedures document resilience and recovery measures in critical processes and act as training and awareness materials providing instructions for business continuity purposes, for example, if key people are unavailable. Measuring procedural coverage implies knowledge of operational processes, which can involve a lot of work, although it may help to prioritize the assessment according to the criticality of the operations. The quality of procedures can be assessed by the ability of an untrained person to follow the instructions and achieve the desired outcomes.

Example Security Metric 5.5

Comprehensiveness of security policy coverage	P	R	A	G	M	A	T	I	C	Score
	75	82	92	78	80	70	73	60	81	77%

Here, we check for the presence of information security policies covering all *necessary* areas howsoever determined by the organization. The exercise of drawing up and

Tip: In conjunction with policy owners, look hard for gaps, overlaps, conflicts, and contradictions. Take the opportunity to revise the wording where necessary to clear these up, following the organization's process for changing, authorizing, and releasing its policies.

Tip: Generic public security standards generally offer good advice but, by themselves, don't necessarily cover all your specific security requirements. Ideally you should draw on standards and other sources, including contractual obligations (such as PCI-DSS if you handle credit card data and contracts or service-level agreements with business partners and customers), plus privacy laws, SOX, company laws, industry regulations, and so forth, to develop and then proactively maintain a comprehensive suite of requirements. That is a major undertaking for someone, but it has obvious benefits in terms of both policy/controls coverage and compliance. It also hints at other valuable metrics.

maintaining the coverage map underpinning this metric is valuable in its own right and is another indicator of a mature approach to information security management.

Example Security Metric 5.6

Policy coverage of frameworks, such as ISO/IEC 27002	P	R	A	G	M	A	T	I	C	Score
	70	75	90	69	85	76	72	65	85	76%

{Metric 5.6} is similar to the previous one, but the benchmark for comparison in this case consists of one or more externally defined generic information security frameworks, models, or standards that have been accepted or adopted by the organization.* To what extent do the organization's information security policies cover the issues raised in the generic guidance?

Because this and the previous metric are measuring such similar issues, we would be surprised if the PRAGMATIC scores were markedly different. Looking a little closer, however, we see there *are* minor differences in the ratings.[†] The previous metric scores higher on Relevance because coverage is assessed against management's view of the organization's ideal policy landscape, whereas the generic standards that are the comparator for {metric 5.6} may not fit the organization's needs

* The ISO/IEC 27002 structure that we use to categorize the example security metrics in this very chapter, for instance, is more than just a convenience. The standard is generally accepted as being reasonably comprehensive and yet flexible. The international committee of experts that developed ISO/IEC 27002 made sensible though arbitrary decisions on the placement of change controls, for example, within the standard. The upshot is that we can gloss over such taxonomic considerations and claim to be following good security practices by referring to the standard.

[†] Don't forget that metrics, including metametrics, are decision support tools that achieve nothing by themselves. It is up to management to interpret and make use of them. When it comes to choosing between metrics with very similar scores, let managers earn their salaries by making the decisions based on their experience/gut feeling rather than insisting slavishly that they stick to the numbers!

Tip: A metric such as this forces you to review your policies periodically and perhaps identify those that are no longer relevant and so can be retired. The metrics process has potential value above and beyond the resulting measurement itself.

quite so well. At the same time, having to define the policy landscape makes the previous more **Costly** than this one.

Example Security Metric 5.7

Number or proportion of security policies addressing viable risks	P	R	A	G	M	A	T	I	C	Score
	65	76	91	73	83	77	70	61	78	75%

If there is no viable or conceivable threat, exposure, vulnerability, and/or business impact, there is little chance of an information security incident. Hence, a policy (or, in fact, any other form of control) is probably superfluous in that case. This metric forces a review of the risk foundation for the policies. If you can find and eliminate unnecessary policies and controls, you will be reducing complexity and cutting costs while, at the same time, encouraging more focus on the remaining policies and controls that actually matter.

The metric might be presented as a proportion that we hope approaches 100% (policies that have yet to be fully assessed or those where the threats are unclear, uncertain, or disputed detract from full scale in practice).

Example Security Metric 5.8

Quality of security policies	P	R	A	G	M	A	T	I	C	Score
	80	85	40	66	72	75	80	80	80	73%

The authors of this book have enjoyed many happy hours discussing the true meaning of quality. For one of us, quality is an innate characteristic (i.e., it is an inherent characteristic), whereas the other considers quality primarily in terms of fitness-for-purpose (i.e., it is in the eye of the beholder). We suspect you may get into similar discussions if you adopt a quality metric whether it happens at the time the metric is designed, when it is implemented, or when it is reported (and perhaps all three!).

Regardless of our ongoing discussion, we agreed that improving the quality of security policies is a legitimate and worthwhile objective. Measuring the quality enables systematic improvement, for example, by setting discrete targets (e.g., all security policies and related materials should achieve a quality rating of at least “acceptable”).

Tip: You may enjoy the discussion and find it worth the effort to reach consensus, so defining a set of quality criteria for the purposes of measuring the quality of your information security policies (or the associated strategies, standards, procedures, guidelines, etc.). Alternatively, you could shortcut the arguments and embrace the ambiguity by asking the users of said policies, etc., to rate their quality as understood in their own terms, using suitable customer feedback/opinion surveys (e.g., see Appendix D).

Example Security Metric 5.9

Percentage of policy statements unambiguously linked to control objectives	P	R	A	G	M	A	T	I	C	Score
	92	91	64	60	85	65	45	75	75	72%

If the objectives for information security policies are not identified (e.g., through compliance criteria or axioms), what are the policies aiming to achieve, and how will you know whether you have or have not achieved them? Clarity of objectives is essential and distinguishes excellent policies from mediocre ones. It drives the definition of policy statements and controls addressing the defined objectives in order to reduce risks. It also helps with the design, testing, implementation, operation, and maintenance of controls. It also provides the basis for an important metric—that is, the extent a control meets the control objective.

Example Security Metric 5.10

Thud factor (policy verbosity/red tape index, waffle-o-meter)	P	R	A	G	M	A	T	I	C	Score
	82	80	60	60	70	45	85	86	84	72%

Tip: The wording of the example metric is less than perfect. Determining whether policy statements are “unambiguously linked to control objectives” sounds like a tedious and subjective process, depending on who does it and how he or she interprets ambiguity. The low Timeliness rating reflects the slowness of the policy drafting, review, and approval processes on the assumption that the metric is measuring issued policies and identifying issues that would need to be addressed. If, however, we are able to identify and address such ambiguities directly during the drafting process, the metric becomes a more Timely and valuable tool.

Tip: Things do change, both in information security and in the business, so specify sensible review/re-approval periods in your security policies, procedures, etc., to avoid them becoming stale and outdated. Having done that, this metric is a breeze.

This may seem a frivolous example, and perhaps it is, but there is a genuine concern here. The thud factor measures the number of audio decibels recorded at a 1-m distance when the entire stack of security policies is dropped onto concrete from a height of 1 m. The point is to discourage the creation of lengthy, verbose, confusing, or overlapping policies that are less likely to be read, understood, and complied with. Policies (specifically) should ideally be very succinct statements of management intent and direction, thereby clarifying management's expectations for governance, risk management, and security/control. Red tape and waffling are distinctly unhelpful.

Example Security Metric 5.11

Number of security policies whose review/re-approval is overdue	P	R	A	G	M	A	T	I	C	Score
	54	88	92	14	97	77	43	90	89	72%

This straightforwardly points out how many security policies have not been reviewed and (if appropriate) re-approved on time. "Overdue" implies that review/re-approval is due at some defined point, of course, and that there is a process for reviewing and re-approving them.

The **Genuine** rating takes a big hit because of the possibility of people claiming to have reviewed policies when they haven't or perhaps carelessly re-approving policies that should really have been revised or dropped, simply to get the metrician off their backs.*

Example Security Metric 5.12

Flesch readability scores for information security policies, etc.	P	R	A	G	M	A	T	I	C	Score
	68	77	60	86	35	70	64	88	41	65%

Ostensibly, an easy way of measuring the readability of security policies and, perhaps, related documentation has a certain attraction. The fact that products

* On reflection, we must have been in a rather cynical frame of mind when we rated this metric! It's also possible we made a typing error when recording the rating for **Genuine**. We left it unchanged in the book as an excuse to add this footnote encouraging you to go back over your own ratings and notes before you finalize and publish the scores, especially if you have been rating lots of metrics in one marathon sitting (not a good idea). We're only human.

Tip: Policies, standards, procedures, and guidelines are generally intended for different audiences with differing readability requirements; hence, it is not necessarily appropriate that they should all possess the same level of readability. Furthermore, the formal language typical of policies, in particular, is a style cue that reinforces their nature as the official organs of management edict.*

* The use of archaic language and stilted pseudo-legal phrases (legalese), such as “including, but not limited to” in policies is often taken too far, however, to the point that it interferes with comprehension by the very people who are expected to comply with them. The aforementioned clause should not be forgotten!

such as Microsoft Word can automatically measure (or, strictly speaking, estimate) readability by assigning a Flesch score gives this metric the advantage of being simple to generate. In reality, however, it takes a finite time to open each of the documents, assess them, and note the scores (so the Cost of the metric is not trivial), and then it's not entirely obvious what the scores Mean nor how to Action them, that is, exactly how to adjust the materials to make them more readable without losing the plot.

Example Security Metric 5.13

Number or proportion of security policies that are clear	P	R	A	G	M	A	T	I	C	Score
	75	70	68	41	96	50	56	90	34	64%

This metric scores a bit below {metric 5.12} mostly because it lacks the objectivity of Flesch scores or whatever; hence, it is less Genuine. At the same time, clarity of policies is arguably not quite the same thing as Flesch scores. Clarity certainly needs less explanation than Flesch scores, so {metric 5.13} scores much better than {metric 5.12} on the Meaningful criterion.

Example Security Metric 5.14

Percentage of security policies that satisfy documentation standards	P	R	A	G	M	A	T	I	C	Score
	66	47	79	45	74	38	44	50	35	53%

{Metric 5.14} is typical of rather stilted, formalized metrics that match the classic definition of red tape. The very mention of documentation standards hints at a corporate environment in which things must be done by the book (literally). We are not arguing that structure, order, and formality are necessarily bad, rather

that they have their place. Policies *are* formal documents, and, as such, there are benefits in having common layouts and styles that suit their purposes, but there are limits to this. Sometimes it is entirely appropriate for policies, etc., to break with convention. The odd diagram and splash of color can certainly add impact—and that may be more important than the corporate policy style guide (volume 3a).

Example Security Metric 5.15

Number of security policies that are inconsistent with other policies or obligations	P	R	A	G	M	A	T	I	C	Score
	60	49	76	43	88	45	41	43	12	51%

Inconsistencies* between policies, laws, regulations, procedures, guidelines, work instructions, training materials, and so forth are obviously best avoided, so it kind of makes sense to count and report them in order to drive them down. On the other hand, the real value comes from identifying and addressing the inconsistencies, rather than reporting them per se, so this is an example of a rather pointless metric. The effort and expense involved in the metric is arguably better spent on finding and fixing the issues, which is why it scores so badly for Cost.

7.3 Security Governance, Management, and Organization Example Metrics

Management of an information security department, program, or function is not substantially different from managing any other organizational department. However, we lack the decades of history and study on effective security management practices. Furthermore, most information security managers, IT security managers especially, come from technical/IT, rather than management, backgrounds. But the key difference is that managers in most other departments have good metrics to guide them and inform senior management about their effectiveness.

So how do we gauge a successful security manager or, indeed, determine whether a security manager is as successful as he or she appears to be? How does senior management know if the security manager is truly earning his or her keep? What is the basis for performance reviews?

These are sound reasons to develop information security management and governance metrics. While the field, at first, appears somewhat nebulous, we consider quite a range of measurement criteria and approaches in this section.

* Notice that this metric is worded in a negative sense—it might have scored slightly better if it reported the number of policies that were *consistent*.

7.3.1 Information Security Financial Management Metrics

Substantial investments in security controls need to be financially justified in the same manner as other corporate investments, not least because they are usually competing for the same financial and other limited resources. If investment proposals of any type are not adequately justified, they are unlikely to receive approval, support, or budget.

Most organizations run on numbers—particularly dollars in commercial companies. The absence of good financial analysis of security activities is frequently blamed for the lack of management support. The information security manager needs to appreciate that deciding whether to spend a million dollars on security or on developing a new market or product is typical of the choices confronting business management. Absent a convincing dollars-and-cents business case for investing in security with a reasonable prospect of a decent return or an obvious and pressing compliance requirement, the typical information security project is sadly not the most obvious or sensible way to spend the organization's cash.

By the way, contrary to the expressed wisdom in some information security circles, projects that will cut or avoid costs are every bit as valuable and “profitable” as those that will generate additional income. This is accounting 101. We have already mentioned the value equation: financially speaking, it makes no appreciable difference whether an investment of $\$X$ creates $\$Y$ of additional income or saves $\$Y$ of anticipated costs. The net value in both cases is $\$Y$ minus $\$X$.

7.3.2 Information Security Control-Related Metrics

Control metrics are essential because controls are what we rely on to mitigate unacceptable risks. How effective is information security likely to be if we have no feedback—no measurements—telling us how good our controls really are? If our security controls aren't sufficient and effective, we are deluding ourselves if we believe we have contained the risks. *We're not managing; we're just guessing.*

A stack of important but rather awkward questions from management relate to the information security controls:

- Are the information security controls in fact operational and working correctly?
- Are we actually controlling what we think we're controlling?
- How often and under what circumstances can our controls fail? Would we discover they had failed *before* an incident occurred? What are the likely consequences if this happens? What's the worst-case scenario?
- How good do our security controls realistically need to be? Do we need to divert resources from some other part of the business or can we afford to slacken off a bit?

- In what manner can we most effectively improve our security controls? How could we do it better?
- Are all our information security risks adequately mitigated, or are there things that would keep me awake at night if only I knew?

When not unreasonable questions such as these are asked of those responsible for information security, the usual response is a blank, bunny-in-the-headlights stare and maybe an incoherent splutter about best practices (whatever that means!). The information security manager with PRAGMATIC metrics has a natural advantage, not just in being able to respond sensibly to management's questions and back up the responses with relevant data* but also, in fact, having a tool to manage information security risks rationally and systematically.

Absent defined control objectives, what is the basis for control design, and how can we develop relevant metrics? After all, the primary metric for controls is to what extent they meet the objectives.

Control objectives must be carefully crafted to ensure they actually achieve the desired level of risk management and outcomes. If there is uncertainty about appropriate objectives, there are a number of good sources, such as the ISO27k standards or COBIT from ISACA. These can be reviewed for relevance to the organization and also from the perspective that compliance with such objectives is not usually binary. That is, even relevant control objectives may not need to be 100% realized to achieve an adequate level of control for a particular organization. Because greater control is usually accompanied by increased costs in time, money, or convenience, there will be a tipping point beyond which the cost of greater control exceeds the benefit, and so is not cost-effective.

In addition, the degree of appropriate control needs to be considered in light of the organization's capabilities to respond effectively to control failures that result in compromises and other incidents. Arguably, the more effective the organization's incident response capability becomes, the lower/less restrictive the control objective can be. The rationale is similar to needing less fire insurance if you live next to the firehouse.

7.3.3 Metrics for Business Alignment and Relevance of Controls

Any control objectives and, hence, any uniquely associated controls that lack justifiable business purposes are not relevant to the organization. In ISO27k terms, they are identified on the organization's statement of applicability as being unnecessary and out of the scope of the information security management system. Measuring

* Not necessarily providing absolute demonstrable proof, though surely better than mere assertions and fluff!

the extent of business-control alignment is a highly useful exercise and should be of considerable interest to management and business owners.* Alignment is a major component of the business case for information security as it determines the demand element of the value proposition for security controls. Why on earth would we employ a security control that doesn't serve some valid business function, such as protecting an information asset that requires such protection?

Control relevance is similar to the issue of alignment. The question is whether whatever the control controls actually needs to be controlled. Bear in mind that controls tend to develop organically over time (decades perhaps), and once embedded in the fabric of the organization, they never seem to die a natural death even when completely useless. These ossified controls become just the way we do things around here even if nobody can remember why or what their purpose is. And often the status quo bias translates into "if it ain't broke, don't fix it," perpetuating unnecessary and potentially wasteful activities.

Relevance is seldom a binary state: a given control may be partially relevant to a given control objective or business/security need, perhaps supporting or complementing other controls (auditors may refer to these as compensating controls that are not ideal but compensate for weaknesses or gaps that other controls leave behind). Again, a matrix relating controls to objectives can help identify controls that are not earning their keep as well as gaps in the matrix.

7.3.4 Control Monitoring and Testing Metrics

The extent to which controls are effectively monitored is a useful key performance indicator when developing or improving the security program. If controls aren't being monitored, how do we purport to know if they are working? This issue arises because systems and processes don't stay static for long. Changes, such as software updates, new business processes, new personnel, etc., sometimes disable, undermine, or bypass controls.

The extent controls are *tested against the control objectives* (assuming the control objectives exist and are in fact rational) is another good indicator of security maturity. Are important controls checked/tested and confirmed regularly? Does the organization even appreciate that some controls are more important than others? Are the security controls and functions adequately tested against the security-related specifications (e.g., use and misuse cases) when new IT systems are being implemented or modified? The coverage, nature, and outcome of controls testing will generate worthwhile metrics.

* A useful measure of an organization's security maturity is the extent to which security controls are linked to control objectives, such as those delineated in ISO27k, and conversely, how many control objectives are incompletely or, in fact, excessively addressed by controls. A matrix relating controls (on one axis) against control objectives (on the other axis) is one way to identify the associations and identify any gaps or imbalances.

		PRAGMATIC Ratings (%)						
		Score			Cost			
		Independent		Timely	Accurate		Meaningful	
		Actionable	Relevant	Predictive	Strategic, Managerial or Operational	S M O	S M O	S M O
Information Security Management and Governance Metric		6.1 Quality of security metrics in use	S M	96	91	99	92	88
6.2 Percentage of security controls that may fail silently		S M O	90	90	90	90	93	86
6.3 Security governance maturity		S M	95	97	70	78	91	89
6.4 Information security ascendency		S	97	87	15	94	86	90
6.5 Percentage of controls unambiguously linked to control objectives		M	92	91	64	60	85	65
6.6 Number of controls meeting defined control criteria/ objectives		M O	88	86	88	65	78	60
6.7 Proportion of critical controls consistent with controls policy		S M	83	92	80	83	89	82
6.8 Corporation's economic situation		S M	72	80	10	80	80	80
6.9 Percentage of controls that are ossified or redundant		S M	85	88	85	80	84	75
6.10 Control objectives tied to specific business objectives		S M	96	95	65	55	99	50
6.11 Days since the last serious information security incident		M	62	70	11	87	87	10

6.12	Annual cost of information security controls	S M	94	92	90	77	97	44	50	16	20	64%
6.13	Number of different controls	S M	71	75	72	75	88	30	50	65	43	63%
6.14	Extent of accountability for information assets	S	94	93	78	36	72	76	30	40	37	62%
6.15	Information security expenditure	S M	82	94	60	60	89	29	33	49	59	62%
6.16	Benford's law	O	84	30	53	95	11	98	62	98	23	62%
6.17	Net present value (NPV)	M	77	72	25	35	85	55	44	60	88	60%
6.18	Return on investment (ROI)	M	70	72	25	30	82	50	44	60	88	58%
6.19	Internal rate of return (IRR)	M	69	72	25	30	82	50	44	60	88	58%
6.20	Payback period	M	65	72	25	25	88	50	44	60	90	58%
6.21	Information security management customer satisfaction rating ^a	S M	60	60	40	35	85	51	85	15	80	57%
6.22	Information security controls coverage	M O	87	89	65	40	74	35	46	40	30	56%
6.23	DEFCON level	M	5	10	30	85	25	71	88	90	91	55%
6.24	Controls consistency	M	78	83	67	60	71	33	27	31	27	53%
6.25	Scope of information security activities	S	86	74	35	44	70	37	30	44	45	52%
6.26	Value at risk (VaR)	M	70	65	20	30	35	40	30	30	22	38%
6.27	Return on security investment (ROSI)	M	40	40	20	20	55	45	25	40	30	35%
6.28	Security budget as proportion of IT budget or turnover	M	13	3	16	2	2	0	4	18	88	16%

^a This is the example metric from the previous chapter.

Example Security Metric 6.1

Quality of security metrics in use	P	R	A	G	M	A	T	I	C	Score
	96	91	99	92	88	94	89	79	95	91%

Forgive us for including this rather self-referential metric, but we believe the quality (as in inherent quality, suitability, and fitness for purpose) of the organization's information security metrics has a *huge* bearing on the way it governs and manages its information security. The PRAGMATIC metametrics approach fits the bill as a way of assessing and scoring the quality of the metrics and, hence, is a valuable metric in its own right.

Example Security Metric 6.2

Percentage of security controls that may fail silently	P	R	A	G	M	A	T	I	C	Score
	90	90	90	90	90	93	86	93	80	89%

This is an intriguing metric concerning an insidious and seldom-recognized threat. Most of us blithely assume that the security controls we recommend and install work properly (provided they were properly implemented, of course) and will continue to do so indefinitely. In reality, even assuming they work correctly in the first place, which is far from certain, security controls sometimes fail in service for a variety of reasons mostly associated with change:

- The emergence of novel threats or modes of exploitation
- Additional vulnerabilities exposed as a result of technical/platform changes
- Configuration changes that accidentally disable or negate controls
- Business changes affecting the business impacts of security incidents

The information security profession's curious faith in the security controls represents a serious blind spot.

This is another indicator of security maturity. The rationale is blindingly obvious: unmonitored controls may decay or fail without this being noticed, silently increasing the risk. Organizations with relatively immature information security management tend not to have the impetus or the resources to conduct the requisite amount of monitoring, other than perhaps testing (some) controls when initially implemented or selectively during (certain) audits (e.g., Sarbanes–Oxley Act (SOX) auditors may sample a few of the security controls protecting the integrity of SOX-relevant IT systems).

Tip: The frequency or periodicity of monitoring ought to reflect the significance or criticality of the controls—for example, safety- or business-critical controls that absolutely must not fail deserve to be monitored constantly as well as being fail-safe and triggering appropriate responses if they ever should fail. Less critical controls (those with less significant impacts if they fail) may be tested/checked less often. How long since yours were checked?*

* Average number of days since critical security controls were last checked might be a similar metric.

Example Security Metric 6.3

Security governance maturity	P	R	A	G	M	A	T	I	C	Score
	95	97	70	78	91	89	90	85	90	87%

Once again, we envisage a metric based around a maturity scale and scoring matrix, such as that in Appendix H. However, that is not the only approach. Here is an alternative. Most would probably agree that an effective information security governance structure will encompass attributes such as the following (ISACA 2012):*

- A security strategy with senior management acceptance and support
- A security strategy intrinsically linked with business objectives
- Security policies that are complete and consistent with strategy
- Complete standards for all relevant, consistently maintained policies
- Complete and accurate procedures for all important operations
- Clear assignment of roles and responsibilities
- An organizational structure ensuring appropriate authority for information security management without inherent conflicts of interest
- Information assets that have been identified and classified as to criticality and sensitivity
- Effective controls that have been designed, implemented, and maintained
- Effective security metrics and monitoring processes in place
- Effective compliance and enforcement processes
- Tested and functional incident and emergency response capabilities
- Tested business continuity/disaster recovery (DR) plans

* Some might scoff at using CISM exam review material as a reference, and while it may not represent the veritable cutting-edge of information security sophistication, it does arguably represent the largest global consensus of practicing, in-the-trenches information security managers—more than 13,000 as of this writing.

- Appropriate security approvals in change management processes
- Risks that are properly identified, evaluated, communicated, and managed
- Adequate security awareness and training of all users
- The development and delivery of activities that can positively influence security orientation of culture and behavior of staff
- Regulatory and legal issues understood and addressed
- Addressing security issues with third-party service providers
- The timely resolution of noncompliance issues and other variances

A crude but arguably effective metric involves someone simply scoring the organization against each item on a scale from nonexistent (score 0) to fully in place (score 5). If nothing else, it will give management a clue about where their strengths and weaknesses lie with respect to information security management.*

Example Security Metric 6.4

Information security ascendency	P	R	A	G	M	A	T	I	C	Score
	97	87	15	94	86	90	99	97	99	85%

Organizational structure (in the sense of where information security fits into the scheme of things and its scope) is a decent measure of the organization's security maturity. The reporting level, we believe, is a particularly strong indicator of senior management's appreciation of the importance of information security to the organization.

In some traditional/old-fashioned organizations, information security is buried down in the depths, typically reporting to the IT manager, CIO, or even operations.[†] As such, it is considered a necessary evil—a technical function performing largely administrative duties (password resets mainly!), a cost center or sinkhole offering marginal, if any, business benefits. Sometimes it only exists as an afterthought, perhaps a response to regulatory mandates. This metric therefore simplistically (and Cheaply!) counts the number of hierarchical levels or layers of management between whoever sits at the peak of the organization's executive management (normally the CEO or president) and the most senior person explicitly accountable or responsible for information security (the person we're calling the information

* Because most of these elements won't exist in isolation and tend to be related, it seems likely that a few will be indicative of the overall situation. We might consider taking a shortcut, perhaps considering only the first six items on the list. It does not seem unreasonable to assume that if those six are sound, the balance of the list will be in pretty good shape...but take care with such assumptions as they can seriously affect the Accuracy and credibility of any metric. We can't say whether that will matter, but be careful with shortcuts.

[†] Management guru Peter Drucker pointed out that for every additional layer of management, the noise doubles and the amount of information is halved, causing a 6-dB reduction in the signal-to-noise ratio for the engineers among us.

Tip: Hierarchical levels can be indistinct and difficult to count in matrix management situations. If your organizational chart is a confusing tangle of solid and dotted reporting lines or if it is hard to pin down exactly who is the most senior information security person, that, in itself, would seem to indicate a lack of accountability. Nevertheless, it is usually possible to assess the hierarchical status of information security management relative to, or in comparison with, corporate functions, such as finance, production/ops, or sales that are generally considered powerful and influential. A relative score or rank is a valid metric and may beneficially be compared to peer companies.

security manager for convenience, but it could be a CISO, CSO, CRO, security director, or VP of security, security analyst, or security guru).

The very low Actionability score reflects the near impossibility of anyone except senior management changing reporting relationships and organizational structures. If the metric indicates information security is buried at too low a level in the hierarchy (compared to peers), the information security manager is unlikely to have the power, influence, or credibility to be promoted more than one level without some heavyweight help from above—and even then, feathers will definitely be ruffled. A more likely response is for management to appoint someone with the necessary credentials directly to a new senior role.*

Example Security Metric 6.5

Percentage of controls unambiguously linked to control objectives	P	R	A	G	M	A	T	I	C	Score
	92	91	64	60	85	65	45	75	75	72%

The rationale here should be obvious: information security controls for which there are no corresponding control objectives appear to be unfounded and, hence, may be unnecessary. What risks are they meant to address? Are there, in fact, valid requirements or concerns to justify keeping the controls, or can they be dropped?

The metric is Actionable through either defining and documenting/clarifying valid control objectives or retiring unjustified controls. The metric may require some interpretation and explanation in order to be Meaningful to management, but mostly, the discussion is likely to center on identifying and withdrawing security

* Information security reporting to the head of IT or the CIO represents a fundamental conflict of interest and, as they say in the insurance industry, a moral hazard. During 2011, for example, Sony Network Entertainment International (SNEI) suffered an extremely embarrassing and very public series of hacking incidents on PSN, the PlayStation Network. It was surprising that a technology company would appear so ill-equipped to deal with such an obvious threat, but even more astonishing was the eventual company announcement that SNEI had created the new role of CISO, reporting to the CIO of its parent company Sony Corp.

Tip: Killing off unnecessary security controls cuts costs, reduces complexity, and is thus *a good thing* for the organization if rather awkward for most information security and risk management professionals who are more accustomed to introducing new controls. It can be a cathartic experience to identify lame controls, determine whether any still have value and so are worth patching up, and finally put the remainder out of their misery. Don't forget to keep notes about the savings, which may one day come in useful to demonstrate that information security management truly reduces the organization's costs.

controls that are no longer needed, typically because of changes in the business situation, information security risks, or compliance obligations. Sometimes you may find that certain controls have been superseded by others. Occasionally, you may identify controls that simply did not work out in practice. More often, when it comes to examining them in detail, nobody can recall for sure what the controls were ever meant to achieve!

Example Security Metric 6.6

Number of controls meeting defined control criteria/objectives	P	R	A	G	M	A	T	I	C	Score
	88	86	88	65	78	60	26	90	70	72%

If controls don't meet their defined/designed criteria or objectives, the solution is patently either to improve the controls or to review and adjust or restate the objectives. We assume this metric would be reported periodically, so its Timeliness score depends on the testing-and-reporting interval.

Example Security Metric 6.7

Proportion of critical controls consistent with controls policy	P	R	A	G	M	A	T	I	C	Score
	83	92	80	83	89	82	32	70	35	72%

Tip: Whereas, on the whole, we tend to prefer metrics that report percentages or proportions, straightforward counts are most useful when it is clear that the ideal proportion is 100%: the count tends to give management a better feel for exactly how much work remains and can be especially motivational when it gets down to the last few. This is a pragmatic application of human psychology!

Tip: This is an example of a *clever* metric, perhaps too clever for its own good. Ostensibly the metric should drive the controls toward being more consistent with policies. You might even expect it to encourage the development of such policies...but, in practice, it is more likely to generate disputes about which controls are critical. It could easily turn out to be counterproductive if controls are artificially downgraded from critical simply to improve the metric.

An example of a controls policy might be that access is permitted unless expressly forbidden as opposed to access is denied unless expressly permitted. Another would be trust is transitive and can be delegated or perhaps trust no one, verify everything. The example metric assumes such policies are defined and are applicable. It is possible that policies may not be documented or applicable to all controls, hence the focus on *critical* controls on the basis that the criticality of controls has been determined and critical controls are more likely to have associated policies. It is, however, a **Costly** metric.

Example Security Metric 6.8

Corporation's economic situation	P	R	A	G	M	A	T	I	C	Score
	72	80	10	80	80	80	61	80	79	69%

Financial duress within the organization can raise or emphasize novel information security concerns (such as frauds or thefts committed by disillusioned employees or suppliers whose profit margins are squeezed), constrain security budgets, and result in increased pressure to cut back on any security controls that are perceived as being relatively expensive or at least not sufficiently cost-effective.

Conversely, substantial profits, new investments in the organization or management's burgeoning optimism, may result in the relaxation of normal financial controls and a tendency to invest heavily in a multitude of projects without, necessarily, adequate attention to project management. Fast-growing organizations don't have time to implement and test proper controls and are often rather chaotic. In such circumstances, the information security risks of significant changes are not always taken adequately into account, and the preexisting information security management resources may not cope well with mushrooming demands on their expertise.

Either way, this metric builds on the premise that the organization's economic status has a substantial bearing on its information security capabilities.

Obviously enough, it suffers badly on the Actionability rating because there is not a lot that anyone can do to affect profitability that they aren't already doing! But it does serve as a KRI and suggests heightened alertness.

Tip: There is a risk of removing necessary, valid controls that are declared ossified by mistake, so be careful when taking action as result of this kind of metric!

Example Security Metric 6.9

Percentage of controls that are ossified or redundant	P	R	A	G	M	A	T	I	C	Score
	85	88	85	80	84	75	22	62	39	69%

“Ossified” refers to controls in place that are no longer necessary, have no identifiable business purpose or value, or don’t map to a control objective or viable threat. These are clearly avoidable costs. Removing unnecessary controls cuts the costs associated with using the controls, plus their management and maintenance. It also simplifies the control environment. The main issue with this metric is the challenge involved in locating and verifying ossified/redundant controls.

Example Security Metric 6.10

Control objectives tied to specific business objectives	P	R	A	G	M	A	T	I	C	Score
	96	95	65	55	99	50	40	70	40	68%

The value of {metric 6.10} stems from linking security strategies, control objectives, security policies, and security controls to the organization’s business objectives. Some security practitioners are still confused about their primary function in the business. They labor under the misapprehension that their primary function is to protect information assets from risks, whereas, in fact, the real value of information security management is to make the business as profitable and successful as possible. This is accomplished by minimizing disruptions to the activities that generate revenue. The business objective is simply not going to be achieved by attempting to mitigate every single threat, vulnerability, exposure, and impact. Apart from being literally unattainable, excessive security is costly and generally counterproductive. Alignment with *the business* is every bit as important for information security as it is for any other business function, such as production, HR, IT, or finance.*

The metric itself may not have a stellar PRAGMATIC score, but it does raise the prospect of trimming costs by removing unnecessary controls and refocusing the information security department on the things that actually matter to the business. The metric also implies the existence of a controls inventory, which is a valuable information asset in its own right.

* Imagine a tug-of-war, the corporation against its competitors, where the information security guys are pushing...

Tip: It is probably obvious from our notes that we believe this metric might be a hot one for the information security manager, personally. Although the focus of any metrics project tends to be on finding metrics to suit corporate management, it is also an opportunity to find better operational metrics for the department.

Example Security Metric 6.11

Days since the last serious information security incident	P	R	A	G	M	A	T	I	C	Score
	62	70	11	87	87	10	92	95	95	68%

Despite the mediocre score, {metric 6.11} is an intriguing concept. We envisage a board not unlike the “Days since a lost-time accident” thing that used to adorn the main factory gates. Its purpose was, of course, to raise awareness of health and safety practices and, hence, to improve health and safety. In just the same way, {metric 6.11} could be an interesting information security awareness reminder.

The reality is that “Days since a lost-time accident” boards have mostly disappeared quicker than the Western factories they adorned. It seems to us the main drawback of this style of metric is that it is not Actionable in any specific way without more information about the nature of the incidents. After the initial impact wears off, the metric becomes as bland and meaningless as those DEFCON-type indicators (see {metric 6.23}) until, eventually, it no longer registers at all—a biological process known as “accommodation” or “habituation.”

Example Security Metric 6.12

Annual cost of information security controls	P	R	A	G	M	A	T	I	C	Score
	94	92	90	77	97	44	50	16	20	64%

Management is always concerned about costs; hence, it makes sense to get a handle on them. Tracking costs over time is also useful in gauging efficiency, that is, if we can maintain or increase the effectiveness of controls while reducing costs, we’ll probably increase management satisfaction with our efforts. At first glance, therefore, the metric sounds quite attractive.

Tip: Almost any metric that is reported day in and day out may suffer the same fate unless it truly resonates with the audience and has value to them by informing their decision processes. Try to avoid boring, bland, pointless metrics. Given the choice, go for impact.

We see two significant drawbacks with this metric, however. First is the substantial Cost involved in tracking and accounting for the full range of security controls throughout the business: we are talking about not just the information security department's annual expenditure on salaries and security toys (which is very easily obtained from finance*), but the costs of operating/using, managing, and maintaining security controls that are widely dispersed across the entire organization—things such as the delays and aggravations caused by having to log in all the time and waiting for the antivirus to catch up. Seriously, when you actually look into the effects on productivity of all the information security controls we tend to recommend so glibly, you start to appreciate that security is, in fact, a substantial contributor to the cost base for the organization.[†]

Second, the metric suffers on Independence because the people who are best placed to determine the true costs of information security controls—namely, the professionals in the information security department—are the very same people who stand to benefit from making their work seem far more cost-effective than it genuinely is. It may be feasible to get truly independent opinions from audit, finance, or consultants though.

Example Security Metric 6.13

Number of different controls	P	R	A	G	M	A	T	I	C	Score
	71	75	72	75	88	30	50	65	43	63%

Counting controls sounds easy enough in theory but can get quite laborious in practice. Exactly what constitutes a control needs to be defined and applied consistently when using this metric, for instance, to avoid counting multiple instances of certain controls (such as antivirus installations on desktops and laptops) separately while lumping others (such as firewalls on the same systems) together. The count might be compared to some ideal number of controls, neither too few nor too many. Interpreting the metric can be quite involved but probably a worthwhile process (e.g., we know of a bank that was able to cut 800 of its 1400 security controls; the initial count was surprising enough to persuade management that there would be value in reviewing and rationalizing the controls).

Tip: Counting different types or categories of controls in use tends to be more useful and easier than counting individual installations. Is it sensible to be running six different brands of firewall, for example? Perhaps we could justify running two or three types for defense in depth, but six?!

* Not so fast, Grasshopper: don't forget that "security" as in site security, security guards, and so on, are also at least partly related to information security as are business continuity and substantial chunks of risk management and compliance and IT and...OK, now do you accept the drawback?

[†] If just reading this makes you feel uncomfortable in your seat, you are way ahead of those information security pros who instantly think, "Yes, but just imagine the costs of the incidents if there was no security!" We do, of course, accept that there are costs *and* benefits to security. The metric is about the function being honest and open, for once, on the cost part of that important equation.

Tip: While this may be a soft, very subjective metric, if measured consistently, the trend may still be a worthwhile indicator of progress—or the lack of it—thereby driving improvements.

Example Security Metric 6.14

Extent of accountability for information assets	P	R	A	G	M	A	T	I	C	Score
	94	93	78	36	72	76	30	40	37	62%

How would one measure the extent of accountability for information assets? It seems to us the bullet-point list we gave earlier in this section could easily be turned into a scoring checklist, perhaps even something as simple as one of those “Give yourself a point for each item” self-assessment quizzes from the coffee-table magazines that might be slipped quietly into a management newsletter.*

Example Security Metric 6.15

Information security expenditure	P	R	A	G	M	A	T	I	C	Score
	82	94	60	60	89	29	33	49	59	62%

Most financial metrics are inherently **Relevant** and **Meaningful** to managers who manage by the numbers. Identifiable expenditure on security is obviously part of the value equation: in short, the reduced or avoided financial impacts resulting from an effective security control during its lifetime less the lifecycle costs relating to that security control equals its net value.

Taken as a whole, security costs and net value might appear to be useful for benchmarking the efficiency of information security against other organizations, but the approach is fraught with dangers. The basis for allocating security costs often varies widely between organizations, and the reduced or avoided impacts risk assessment part of the value equation is equally variable. Provided the basis stays the same, however, the figures may potentially be used within a single organization to track the changing costs and benefits of security over time.

* A self-assessment quiz? Surely not! Well, yes actually. OK, we’re being deliberately contentious to point out that it is not necessarily appropriate to insist on rigorous, scientifically based measurement methods in order to gain useful management information. In this situation, for example, the tongue-in-cheek survey may be sufficient to focus attention and hopefully trigger appropriate responses to the issues being measured *without actually analyzing and presenting the measures at all*. In the right circumstances, a simple, cheap, creative approach may be all it takes to prompt respondents to think about the issues being assessed. The awareness effect may actually be worth more than the metric!

Example Security Metric 6.16

	P	R	A	G	M	A	T	I	C	Score
Benford's law	84	30	53	95	11	98	62	98	23	62%

Benford's law is a fascinating theorem based on the expected distribution of digits in certain types of numeric data, specifically the initial digits of numbers output by processes that are expected to generate data in an unbiased and unconstrained fashion. Careful analysis of digits in numeric data sets can reveal anomalous distributions (such as an apparent surfeit of 3s and 4s with a corresponding shortage of 6s and 7s compared to the expected numbers of those digits), indicating a curious bias in the way the numbers were generated. Further analysis to understand *why* the digit distributions are skewed can reveal causes that escape casual observation.* Benford's law has proven useful in financial fraud detection, for example, because fraudsters who create or manipulate/alter numbers to suit their purposes tend to do so in a deterministic, rather than a random way, albeit subconsciously.

7.3.5 Financial Information Security Metrics

We have grouped these financially based security management metrics together for convenience.

Example Financial Security Metrics

	P	R	A	G	M	A	T	I	C	Score
NPV-6.17	77	72	25	35	85	55	44	60	88	60%
ROI-6.18	65	72	25	25	88	50	44	60	90	58%
IRR-6.19	70	72	25	30	82	50	44	60	88	58%
Payback period-6.20	69	72	25	30	82	50	44	60	88	58%
VAR-6.26	70	65	20	30	35	40	30	30	22	38%
ROSI-6.27	40	40	20	20	55	45	25	40	30	35%

NPV, payback period, ROI, and IRR comprise this subgroup of metrics concerning the projected value of proposed information security investments. The Costs of calculating these metrics (in practice, probably just one or two of the set) are minimal if the organization already uses them routinely to assess other investments. They differ slightly in the ways they are calculated, but unless you are an

* Analyzing our PRAGMATIC ratings would probably reveal a distinct skew toward numbers ending in 0 and 5 because of the way we often start by assigning rough ratings (multiples of 5), then refine most of them later. Sorting the master list of metrics by the individual rating columns, one at a time, helps by letting us check and adjust the ratings and hence the rankings on each criterion (ensuring that the relatively expensive metrics are indeed toward the bottom of the ranking if sorted on Cost, for instance).

accountant or economist, they are sufficiently alike to be treated the same. They are commonly used when developing business cases for projects.

VAR computes the worst probable loss from a compromise at a given level of confidence, typically 95% or 99%. Specifically, it describes the quantile of the projected distribution of losses over a given time period using Monte Carlo simulations based on historical data. VAR is normally used by financial institutions to determine the appropriate levels of cash reserves needed for contingency purposes, but it has obvious implications for managing other kinds of risk.*

ROSI is an ROI method that uses annualized loss expectancy (ALE) and single loss expectancy (SLE) to predict the value that incidents will destroy unless they are prevented. The key problem with this method is that it is extremely hard to determine or assign sensible values for low probability incidents (because we lack the historical basis) even though extreme events may be extremely damaging (“black swans”; Taleb 2010), but for commonplace incidents where we have already accumulated the data (such as viruses and spams), ROSI (or indeed NPV, payback, ROI, or IRR methods) provides a relatively straightforward method of justifying the investment in mitigating controls on the basis of the costs and benefits.

Example Security Metric 6.21

Information security management customer satisfaction rating	P	R	A	G	M	A	T	I	C	Score
	60	60	40	35	85	51	85	15	80	70%

This is the metric we used to illustrate and explain the development and PRAGMATIC rating process in the previous chapter (Section 6.4).

Example Security Metric 6.22

Information security controls coverage	P	R	A	G	M	A	T	I	C	Score
	87	89	65	40	74	35	46	40	30	56%

It is possible to assess the coverage, adoption, or use of information security controls across the organization against good practice standards, such as COBIT,

* Consider, for example, a genuine request from a senior insurance manager to distill information security risk metrics down to a single number, a “risk score.” He or she explains that just as the credit industry relies on a single number credit score, he or she wants to be able to write cyber insurance based on a single risk score—not simply one of the many available risk metrics but *one all-encompassing, all-purpose risk metric*. Considerable time and effort was expended researching the feasibility of developing such a metric, and to an extent, the VAR computation does accomplish this in a fashion insofar as it calculates a maximum loss in a given time period with a stated level of probability. The killer catch is twofold: not only is a great deal of reliable historic data required but also the rates of change have to be limited, conditions unfortunately quite alien to the dynamic world of information security.

Tip: Competent IT auditors can identify strengths, weaknesses, opportunities, and threats in the organization’s information security controls and recommend improvements as well as generating numeric metrics if desired. The trick is to convince audit management of the value of such an approach and to support the auditors in doing their stuff effectively.

ISO27k, SP800-53, and the ISF guidance and potentially other security requirements and compliance obligations. While crude checklists anticipating binary yes/no responses to closed compliance questions may simplify the assessment and scoring, a more open style of questioning that allows “partially” and “not applicable” responses tends to be more useful in the hands of experienced auditors or assessors.

Example Security Metric 6.23

	P	R	A	G	M	A	T	I	C	Score
DEFCON level	5	10	30	85	25	71	88	90	91	55%

DEFCON (defense condition) is simply a well-known example of its type. There are several such indicators; for instance, the SANS Internet Storm Center reports a threat level on a four-point scale (green, yellow, orange, or red). Generic indicators such as these (even if you somehow determine your own corporate equivalent) make mediocre corporate metrics because they are seldom specific enough to be Actionable, partly because the (implied) risks are not often of direct and obvious concern to commercial organizations—they are neither Predictive nor Relevant.

Example Security Metric 6.24

	P	R	A	G	M	A	T	I	C	Score
Controls consistency	78	83	67	60	71	33	27	31	27	53%

Standardization of information security controls (i.e., using the same or similar controls to address the same or similar risks) cuts costs and reduces complexity while increasing the organization’s familiarity with a finite set of controls. Identifying and counting inconsistencies, then, suggests the possibility of rationalizing controls.

Tip: The *transitions* to higher alerting levels can be useful triggers or opportunities to circulate general security awareness materials reminding employees that some external threats are both relevant and serious.

This metric would be quite costly to compile unless your controls inventory is comprehensive, but the analysis could also be done piecemeal (e.g., this quarter review/measure consistency of the authentication controls across the organization, next quarter standardize them...).

Example Security Metric 6.25

Scope of information security activities	P	R	A	G	M	A	T	I	C	Score
	86	74	35	44	70	37	30	44	45	52%

The scope of security activities as related to overall organizational activities can be somewhat useful, especially if tracked over time to underscore trends. Arguably, the greater the scope is, if suitably supported, the more effective security activities are likely to be.

Example Security Metric 6.28

Security budget as a proportion of IT budget or turnover	P	R	A	G	M	A	T	I	C	Score
	13	3	16	2	2	0	4	18	88	16%

Although seemingly not Predictive of nor Relevant to anything much in security terms, hence its abysmal score, {metric 6.28} is Cheap enough that it might perhaps be tracked year-by-year to discover whether there is, in fact, any relation between security budget relative to IT or turnover and security outcomes, particularly incidents.*

Tip: We're only human. Mistakes happen. If you are going to place reliance on the PRAGMATIC process to select your metrics, double-check the numbers and challenge any that seem out of place in the rankings. You may discover typos, or on reflection, you may decide to alter the scores to bring an errant metric back into line with its peers. Sorting the PRAGMATIC tables by each of the columns, in turn, is a good way to find possible anomalies.

* We are hinting this time that even rotten metrics may have utility and value if they reveal unexpected relationships between factors that were not expected to correlate. We are getting into the realm of data mining, which only works in practice with large data sets, not random assortments of metrics. All in all, this metric hasn't got much going for it.

7.4 Information Asset Management Example Metrics

Information asset ownership is a powerful security concept in that it emphasizes responsibility and, in particular, reinforces personal accountability for the protection of valuable information.

The degree to which suitable people (generally quite senior managers) are held *personally* accountable and so take responsibility for information security is, we believe, strongly correlated with the organization's security maturity. Experience, common sense, and studies consistently show that people take more care of the things they "own" than the things they don't. A simple question such as "Who owns the email system?" typically draws blank stares and professions of ignorance, sometimes vague answers such as "Er, well, I guess it belongs to the company" or "IT maybe..." The lack of clarity becomes painfully obvious when doing incident postmortems. Everyone blames the consequences on a host of others and disavows any personal culpability. Management blames underlings (we've heard choice comments such as "Useless bunch!"), staff blames their superiors ("We were simply following orders!"), one department blames another, the organization blames its suppliers. It should be pretty clear that this kind of carrying on is not the sign of a mature security organization. The blame game is symptomatic of a dysfunctional, immature organization not intent on systematic improvement and remedying what's defective but rather behaving like adolescents caught doing something naughty. They live in a state of denial.

In our experience, disappointingly few managers reach, let alone go beyond, the point of nominating owners for their most valuable and important information assets, such as major business systems or databases (where "major" varies widely between organizations). We believe management should explicitly define their expectations of information asset owners—for example, mandating an information asset ownership policy specifying that information asset owners are expected to do the following:

- Classify their information assets using the organization's standardized approach and criteria
- Assess the risks to their assets and determine how to treat them (normally conducted in conjunction with risk and security experts)
- Specify and fund the protective measures normally required to prevent or mitigate unacceptable risks, plus the detective controls, incident management, DR, and contingency arrangements to ensure the continuity of the associated business processes should the preventive controls fail (again, normally under the guidance of subject matter experts)
- Determine access policies, typically by defining the roles for users and administrators who will process and control the information assets
- Ensure adequate protection of the assets by providing adequate resources for information security, passing security responsibilities through to suitable people, roles and functions, and instituting suitable compliance arrangements
- Ultimately accept personal accountability for security incidents that affect the information assets

		PRAGMATIC Ratings (%)										
				Score								
				Cost								
		Independent										
		Timely										
		Accurate										
		Meaningful										
		Genuine										
		Actionable										
		Relevant										
		Predictive										
		<i>Information Asset Management Metric</i>		<i>Strategic, Managerial or Operational</i>								
7.1	Number of orphaned information assets without an owner	M	85	90	97	90	95	85	99	90	91%	
7.2	Information asset management maturity	SM	90	95	70	80	90	85	90	85	86%	
7.3	Proportion of information assets not (correctly) classified	MO	75	75	97	85	90	80	80	80	82%	
7.4	Un-owned information asset days	MO	40	51	84	77	74	86	92	94	82	76%
7.5	Integrity of the information asset inventory	MO	82	66	83	78	80	43	50	66	70	69%
7.6	Value of information assets owned by each information asset owner	M	48	64	78	57	79	38	50	22	26	51%
7.7	Percentage of information assets not marked with the (correct) classification	O	52	53	63	44	62	13	17	87	44	48%

Example Security Metric 7.1

Number of orphaned information assets without an owner	P	R	A	G	M	A	T	I	C	Score
	85	90	97	90	90	95	85	99	90	91%

We have raised the concept of information asset owners a few times already. {Metric 7.1} is a back-to-basics count of the orphaned or un-owned information assets, including those that have never had nominated owners plus those whose owners are no longer on the payroll. Given that nobody is held personally accountable and hence feels responsible for protecting un-owned assets, they may not be sufficiently well protected.

{Metric 7.1} is highly **Actionable**: it is obviously implied that owners should be identified for the un-owned assets. It also scores high for **Independence**, **Accuracy**, and **Genuineness** because information asset ownership is normally very formally and unambiguously defined by management.

Example Security Metric 7.2

Information asset management maturity	P	R	A	G	M	A	T	I	C	Score
	90	95	70	80	90	85	90	85	90	86%

A scale for assessing and measuring maturity of the organization's information asset management practices can be found in Appendix H. A high level of maturity can be summarized as managed and measurable, while a low maturity score can be characterized by an ad hoc, seat-of-the-pants approach. While somewhat subjective, the maturity approach has a number of advantages, such as being easy, straightforward, cheap, and comprehended by most.

Example Security Metric 7.3

Proportion of information assets not (correctly) classified	P	R	A	G	M	A	T	I	C	Score
	75	75	97	85	90	80	80	80	80	82%

Tip: It is hard for a manager to deny that he or she is the nominal owner for an information asset when it's written down in black and white and signed off on by a more senior manager. If he or she has a legitimate argument against it, that is a dispute best left to senior management to resolve. Duck!

Tip: Publishing {metric 7.4} may well provide the impetus for management to ensure the nomination of information asset owners.

Question: If you don't know what's important and what's not, how do you allocate finite security resources to their protection? Answer: You don't or, at least, not very well. Most information in any organization is neither critical nor sensitive (unless subject to excessive paranoia), and it is obviously a waste of resources to protect all of it at a high level equally. The more likely consequence is that the really important stuff is underprotected. So we can state with a considerable degree of certainty that any organization that hasn't undertaken classification is still in the crawling stage from a security perspective and the degree that classification has been accomplished is an excellent metric for security management.

Example Security Metric 7.4

Un-owned information asset days	P	R	A	G	M	A	T	I	C	Score
	40	51	84	77	74	86	92	94	82	76%

While similar to the notion of orphan systems, this metric is slightly different in that we're counting the days that assets are orphaned for reasons such as the designated owner has left or has been given a new set of responsibilities. Because it is pretty much a given that neglected, unloved assets are not likely to get much attention and care, it will correlate well with their increasing degree of vulnerability.

Example Security Metric 7.5

Integrity of the information asset inventory	P	R	A	G	M	A	T	I	C	Score
	82	66	83	78	80	43	50	66	70	69%

An inventory—meaning a list, table, or database depending on its complexity—of information assets is a starting point for protecting them. The inventory identifies the stock of information items that are considered in need of protection. Simply put, how can you be sure all important information assets are adequately protected if you are not even sure which assets are important or what assets exist? At a simplistic level, it sounds easy enough to identify and list information assets, but anyone who went through the Y2K pain of checking IT systems for year 2000 surely appreciates that there are devils in those details. This example metric measures the

completeness, accuracy, and up-to-date-ness of the inventory by whatever means are available—for instance, you may sample and validate the records in the inventory against a sample of information assets and likewise sample some records in the inventory and validate them against the actual assets.

Example Security Metric 7.6

Value of information assets owned by each information asset owner	P	R	A	G	M	A	T	I	C	Score
	48	64	78	57	79	38	50	22	26	51%

<This area intentionally left blank>^{*}

Example Security Metric 7.7

Percentage of information assets not marked with the (correct) classification	P	R	A	G	M	A	T	I	C	Score
	52	53	63	44	62	13	17	87	44	48%

Asset classification comes with its own problems, namely, misclassification. In a blame-oriented culture, the tendency will inevitably be to overclassify assets to avoid being at the pointy end of an accusatory digit. In these cases, there needs to be a process to encourage proper classification. If IT operates on a charge-back basis to the business units, then one compensatory control is to charge more for processing and storing higher classifications. Because this will impact costs to the departments, they are likely to be more careful in the classification process.

7.5 Human Resources Security Example Metrics

Information security is very much a human endeavor. Many of the most serious security threats concern attacks deliberately committed or perpetrated by people such as hackers, malware authors, industrial spies, criminals/terrorists, and fraudsters. Whereas there are many technical vulnerabilities in IT systems, these are

* We are making a point here: without the notes, it is not necessarily obvious how we rated the metric. What made us decide this metric was quite strong on Meaning but weak on Independence? What was our understanding of the metric? What did we like about it, and why? What ideas did we have to improve it? Not only is it hard for *you* to fathom our rationale, but frankly, it's hard for *us* to remember the details without our notes!

generally the result of design flaws and bugs introduced by people, while frauds and social engineering attacks directly compromise people and processes. The impacts of security incidents only really become a problem if and when they affect people—so-called victimless crimes are perceived as being less important, for example. Even incidents that damage corporate reputations could be said to be irrelevant except where they damage brand values and, hence, stock prices and livelihoods. In short, people are the core of information security.

Tone at the top, in other words, the security attitudes espoused by influential senior people, is considered by virtually all assurance and security practitioners to be *highly* relevant to the success of security-related activities. Senior management's support for information security has become an industry mantra, widely accepted as a *prerequisite* for effective security. To a large extent, the tone at the top determines the corporate culture, including security and ethical aspects. Therefore, measuring the tone at the top would seem to be highly worthwhile, and yet surprisingly, it happens extremely rarely in practice, presumably because it is a subjective, soft area that technophiles find awkward to handle. Senior management's attitudes toward information security are highly predictive of the organization's overall security stance, but the measures tend to be subjective. Measurement methods need to be designed carefully using specific criteria where possible and ideally employ independent, objective assessors with no ax to grind.

Culture, defined as a pattern of behaviors, beliefs, assumptions, attitudes, and ways of doing things (Kiely and Benzel 2006), can be a powerful force, resisting certain changes, activities, and behaviors while permitting or encouraging others. Culture often has more impact on security than policies, laws, etc., particularly if the rules are perceived as countercultural, creating cultural conflict or dissonance: in fact, the influence of policies, etc., and acceptance of the need to comply are, to a large extent, culturally determined.

Culture is an emergent property of societies or communities that coexists at many levels:

- National, or rather regional, and racial cultures exist: in some parts of the world, for instance, intellectual property is not respected to the extent that piracy is rife and sometimes appears to be tolerated or encouraged by the authorities who are presumably more concerned with short-term economic prosperity than ethics and international laws.
- Entire industries develop recognizable cultures: the financial services industry, for instance, has grown accustomed to compliance with obligations imposed externally by laws and regulations, while individuals within hierarchical military organizations tend to respect orders from superiors even if they conflict with the laws of the land.
- Organizational cultures partially reflect senior management's formal directives, but they are often more strongly influenced by the behaviors and attitudes of managers and other influential colleagues, leading to the concept

“Do as I say, not as I do.” This can cause real problems if managers mandate security controls (such as screensaver timeouts or email encryption) that they are unwilling to adopt themselves.

- Business units, functions, groups, teams, and families develop their own localized cultures and practices, in much the same way that they laugh at their own inside jokes but are perplexed by inside jokes told by others. Frauds involving collaboration between individuals occasionally flourish in tight-knit communities, negating controls, such as divisions of responsibility.
- Even individuals may be said to express certain cultures, approaches, world-views, etc. Certainly within any community, there will be individuals who vary to some extent from the cultural norms within the bounds of peer pressure and personal belief systems, anyway. Terms such as “nonconformist,” “loner,” and “eccentric” arise because not everyone is happy to comply with cultural cues and norms, sometimes instead forging and expressing allegiance to intersecting cultures or groups.

Culture also has a historical basis. It evolves continuously. Significant past incidents and situations experienced and talked about within a society or community can affect the way individuals within those societies/communities perceive and respond to new situations. If a business has suffered severely as a result of, for example, a malware incident, it is only to be expected that management will become highly conscious of, and probably averse to, risks relating to malware. This is just another way of expressing corporate learning.

Deliberately changing cultures within an organization is one of the most difficult and challenging activities any manager might undertake. Nevertheless, security texts often naively recommend adopting a culture of security as if that gem alone is sufficient advice. Experience makes it abundantly clear that, without senior management buy-in and overt support for security, this is a fool’s errand. Try getting staff to wear ID badges when senior managers patently ignore the rule! But if we endeavor to change culture (and have lots of time and patience to do so), we would be wise to consider metrics in order to establish a baseline and determine whether we are achieving the cultural changes we require. Without this, cultural change is a matter of anecdotes and conjecture.

Organizational events, such as significant budget cuts, right-sizing,* and mergers, are extremely stressful as are personal events, such as marriage breakups, deaths in the family, addictions, and money problems. People react differently to stress-

* A politically correct version of downsizing: the term only seems to be used when there are major layoffs, not during hiring binges. If management thinks staff members are unaware of their word games, they are delusional.

ful situations, but the possibility of some sort of adverse reaction tends to increase under stress. Consider these genuine incidents culled from recent news stories:^{*}

- System administrator left logic bombs
- Programmer installed backdoors to systems
- IT network manager changed the administrative passwords for the network and refused to cede control
- Highly confidential classified military data disclosed to an activist group
- Police officer accused of accepting bribes to hack phones
- Customer data files destroyed by a system administrator's "accident"

Given that incidents of this nature are characteristic of people under extreme stress and are surprisingly common, information security and risk managers are well advised to consider the possible exposures and increased risks to the organization brought about by stress on individuals. Stress-related metrics might be an important detective control or KRI.

Behavioral scientists, psychologists, and sociologists have developed creative ways of observing and measuring the behaviors of people and other animals. In theory, we might set up experimental situations to observe employees in security-related activities, but in practice, less intrusive and cheaper means of data collection are more likely to get approved—examples include surveys and reports from HR systems.

Staff morale and attitudes reflect a generalized corporate issue with some bearing on information security. Demoralized, disillusioned, indifferent, resentful, upset, or angry employees *may* be more likely to create or exploit control weaknesses at work, for instance, in order to get back at their employer. They may act carelessly and selfishly with little regard for their security obligations or the effects of their actions and inactions on others (including colleagues, managers, and customers). Conversely, an upbeat, well-motivated, and generally happy workplace tends to be more productive and compliant. Some sort of marker indicating whether morale is below par/deteriorating or at an acceptable level/improving therefore has potential as a security metric, especially when the organization is under stress as a result of mergers and acquisitions, downsizing or reorganizations, economic duress, or regulatory investigation and scrutiny. Such situations don't usually figure in information security risk catalogs, but they probably should.

* We have deliberately not referenced these stories, mostly because we don't want to lose you back to the daily grind of worrying about information security incident risks when you are here to learn about security metrics! They are not individually significant anyway: stories similar to these arrive in our inboxes every day from excellent sources, such as ISN (Information Security News) run by William Knowles, RISKS-List run by Peter G. Neumann, plus dozens of security and risk-related blogs and news sites on the Web.

		PRAGMATIC Ratings (%)						
		Score						
		Independent		Cost				
		Timely						
		Accurate		Meaningful				
		Genuine		Actionable				
		Relevant		Predictive				
		<i>Human Resources Security Metric</i>						
8.1	Human resources security maturity	S M	90	95	70	80	90	85
8.2	Security awareness level	M O	86	89	86	82	85	80
8.3	Rate of change in employee turnover or absenteeism	S M	60	66	20	85	60	75
8.4	Staff morale and attitudes	S M	88	72	60	75	65	75
8.5	Tone at the top	S M	95	50	57	40	91	45
8.6	Corporate security culture	S M	60	76	55	75	60	60
8.7	System accounts-to-employees ratio	M O	74	67	38	39	68	42
8.8	Opinion surveys and direct observations of the culture	S M	80	80	60	55	75	55
8.9	Help-desk security traffic volumes	O	24	33	16	58	5	35
8.10	Culture/worldview	S M	66	30	10	70	40	56
8.11	Employee turn versus account churn	O	30	30	11	36	44	36
8.12	Organizational dysfunction	S M	75	20	10	60	80	40
8.13	Psychometrics	M O	40	24	0	79	15	55

Tip: Do you know of significantly better metrics in this or indeed any other category? Why not join the discussion forum at SecurityMetametrics.com to discuss them with the authors of this book and our international community of readers and metrics experts? PRAGMATIC security metrics are highly sought after! Help us build a shared metrics catalog!

Example Security Metric 8.1

Human resources security maturity	P	R	A	G	M	A	T	I	C	Score
	90	95	70	80	90	85	90	85	90	86%

Use a scoring matrix, such as that provided in Appendix H, to measure how closely the organization's human security practices approach good practice.

Example Security Metric 8.2

Security awareness level	P	R	A	G	M	A	T	I	C	Score
	86	89	86	82	85	80	69	48	75	78%

Security awareness is an extremely important information security control in its own right as well as supporting many other forms of control. Employees clearly have to know about their security obligations imposed by policies, standards, procedures, laws, regulations, contracts, agreements, and ethics, and it helps security immensely if they are sufficiently motivated to comply willingly.

Security awareness levels can be measured using surveys, Web-based quizzes and tests embedded in learning management systems, feedback forms following security events, and social-engineering tests that usually attempt to fool unaware employees into parting with sensitive information. Web logs from information security management's intranet security zone are a neglected source of data concerning employee interaction with the site: for instance, the number of employees accessing the policies and procedures pages and checking out news stories, briefings, etc., that have been promoted by awareness activities is a guide to how effective those activities have been.

Tip: Do you have an Information Security 101 introductory briefing, orientation/induction session, or awareness goodie pack for new general employees to explain the basics and bring them up to speed on information security? If so, consider incorporating a brief mention about the security metrics that employees are most likely to see, perhaps on information security's intranet site. If you have a special version of the security orientation pack for new managers or IT professionals, you should probably put a bit more effort into explaining the key security metrics for them.

Example Security Metric 8.3

Rate of change in employee turnover or absenteeism	P	R	A	G	M	A	T	I	C	Score
	60	66	20	85	60	80	75	80	91	69%

Sudden changes in employee numbers may signal increased information security risks through loss of key people and their expertise, taking on inexperienced new employees, poor morale, significant organizational changes, growth spurts, mergers/acquisitions, etc.*

Employee turnover is an easily captured piece of information that can serve as a KRI or a metric. HR normally keeps track of this information, so it should be readily available. Precisely what the numbers from HR mean is another matter, however: do they cover only permanent employees joining and leaving the payroll, for instance, or does HR also track the comings and goings of contractors, consultants, temps, student or intern placements, and other pseudo-employees, such as third-party maintenance company employees who work permanently onsite? In this vein, short-term contractors in sensitive positions may pose an elevated risk because they will typically have less loyalty and investment in the organization, so this may be useful to track.

Aside from new hires and leavers, does HR account for internal moves/transfers and promotions/demotions? In organizations with many departments or business units and with multiple layers of hierarchy, internal employee moves occur more frequently than hiring or firing people. From the information security perspective, these are all significant events that may affect information/system access rights/permissions, insider threats, divisions of responsibility, experience, morale, etc. Resentful, demoted, or passed-over employees are sometimes the source of added risk from fraud, embezzlement, or theft, and it may be useful to keep track of these individuals if feasible.

An example of a KRI would be if, say, the finance department experiences three times as many staff changes in one month as the average department; this could be an indication of personnel/management issues in finance and, hence, an information security risk that perhaps ought to be evaluated and addressed. On the other hand, it could simply reflect a one-off event, such as a restructuring that was handled exceptionally well by management. In summary, employee turnover can be a useful indicator of something unusual going on, but someone would need to dig deeper to determine whether there are information security implications lurking beneath the numbers.

* Losses may be the result of management releasing people considered to be security threats, and increases may involve taking on additional risk and security people, so the numbers need to be interpreted!

Example Security Metric 8.4

Staff morale and attitudes	P	R	A	G	M	A	T	I	C	Score
	88	72	60	75	65	75	20	50	50	62%

Morale and attitudes are quite easy for an independent observer or an astute member of a society to recognize but are not so readily measured in a scientific, objective manner. The most common formal measurement approach involves one or more of the many available psychometric tests and methods, such as Organizational Culture Assessment Instrument (OCAI; Cameron and Quinn 1999), Myers-Briggs Type Indicator (MBTI; Myers et al. 1998), or Mayer–Salovey–Caruso Emotional Intelligence Test (MSCEIT; Mayer et al. 2003). The HR department may already be using such measures, often as part of the candidate short listing and final selection process.

Another common technique is to conduct some form of (anonymous)* employee opinion survey. In the hands of trained and competent surveyors/assessors, such methods can generate valuable insight for information security and indeed for general management.

The low Timeliness score stands out in the PRAGMATIC table for this metric. The reason is that by the time morale and attitudinal problems are strong enough to come to management's attention as an information security issue, the organization's security status has probably already materially deteriorated—in other words, this is a lagging metric. The Actionability score is also depressed because poor morale can be a highly intractable issue, especially if the main determinants are outside management's control (e.g., there's only so much the C-suite can do to halt and reverse a global economic meltdown!).

Tip: Aside from more scientific approaches, information on morale and attitudes can be obtained cheaply by keeping an ear to the ground, paying attention to rumors, monitoring snarky emails or tweets, and picking up on commentary in forums and social networks (including that old favorite: coffee machine gossip). Simply moving around the organization chatting with various individuals will give most managers a fair picture of the situation, but management by wandering about (MBWA) is highly subjective and not so effective for presentation to higher-ups, although incisive anecdotes from the trenches may be as motivating as the fancy graphs in persuading management that something must be done.

* Aside from the odd outspoken, reckless, or sociopolitically inept individual, most employees will not voluntarily expound on “what’s wrong with this %#\$^&% organization” in any attributable way for fear of recrimination. Provided you are prepared to deal with the angst and issues such surveys may reveal, anonymity dramatically improves respondents’ honesty and encourages them to open up.

Example Security Metric 8.5

	P	R	A	G	M	A	T	I	C	Score
Tone at the top	95	50	57	40	91	45	50	25	70	58%

A simple metric or indicator would be the frequency that top management makes itself available to say a few words at security staff meetings. Another would be managers' compliance with security requirements, such as openly displaying their employee ID badges while on company premises. This could be measured by physically checking, say, the five top managers for compliance once a week and then generating a quarterly report. It might also help to suggest to noncompliant senior management, politely, that it is unrealistic to expect juniors to comply with the corporate security rules if they don't. Done well, this kind of approach has served in some organizations well, dramatically raising compliance, demonstrably improving the tone at top, and hence reinforcing the security culture.

Example Security Metric 8.6

	P	R	A	G	M	A	T	I	C	Score
Corporate security culture	60	76	55	75	60	60	10	75	20	55%

Again, surveys or studies can evaluate levels of interest, support, and drive for information security, typically comparing different departments/business units or levels of the hierarchy (e.g., contrasting the security culture between managers and staff). For example, if the results of a survey indicate a weak security culture, management might support additional security awareness and training activities to address this. Repeating the survey some months later will indicate how successful those activities have been. Successive surveys might focus on different aspects of security, for example, policy compliance, incident reporting, etc.

The Accuracy largely depends on how scientifically it is conducted and the Independence of the surveyors. Using a specialist team of surveyors will improve both aspects but will cost more and could be more disruptive. In other words, you have multiple choices in the design and execution of this kind of metric.

Example Security Metric 8.7

	P	R	A	G	M	A	T	I	C	Score
System accounts-to-employees ratio	74	67	38	39	68	42	36	83	44	55%

Tip: On the basis that what gets measured gets done, simply measuring and reporting this metric should focus attention on it and thereby improve the situation somewhat.

Tip: Opinion surveys and direct observations are applied psychological and sociological research techniques and normally involve the use of trained psychologists, making them relatively expensive. They can also be very intrusive. Online surveys may be less scientific, but they are generally cheaper, and employees can respond when it suits them. A prize of nominal value may be all it takes to get a statistically valid sample to respond, but don't overdo it: people who are surveyed too often become blasé and careless in their responses, saying virtually anything (often responding with what they think you want to hear) just to claim their prize.

This metric is mainly useful if, for example, users are supposed to have only one account each, and the total number of accounts exceeds that number. Otherwise, unless users have many accounts that might increase exposure or the probability that they've written passwords down, it is of limited benefit.

Example Security Metric 8.8

Opinion surveys and direct observations of the culture	P	R	A	G	M	A	T	I	C	Score
	80	80	60	55	75	55	10	45	10	52%

Creating or stimulating a culture of security involves measuring various aspects of the culture in order to determine how much it needs to change and confirming whether activities, such as policies, accountabilities, training, and awareness, achieve the changes desired. A number of approaches to measuring culture directly have been developed over the years, but most are too specialized or intrusive to be of use to the information security manager. Of the various elements of culture noted in the definition earlier, assumptions and attitudes are internalized and hence quite hard to elucidate, whereas expressed behavior is more readily observed and so may be the easiest aspect to measure.

It has been said that culture explains how people behave when they believe they are *not* being watched. If a strong security culture truly exists, employees will be naturally compliant and will try to do the right thing even when the rules are uncertain. Measuring what cannot be directly observed presents something of a conundrum (just ask any theoretical physicist)! A physical security measure for tailgating such as {metric 9.3} might be considered a behavioral trait, potentially an indicator of the state of security culture. Alternatively, we might select a broader metric covering all the security infractions we monitor (perhaps one of those in Section 7.12). Because greater compliance is likely one of the outcomes we're looking for, and, arguably, a security-conscious culture involves following the security rules more diligently, any rule that's relatively easy to monitor could potentially be used as an indicator.

Of course, simply following rules, especially those known to be monitored, may not indicate the state of the organization's culture but may, in fact, be the result of rigorous enforcement. Maybe employees work in fear of being caught breaking the rules. We can't effectively monitor every rule and watch every employee all the time, however, and a culture of fear is every bit as risky as a culture of insecurity.

Example Security Metric 8.9

Help-desk security traffic volumes	P	R	A	G	M	A	T	I	C	Score
	24	33	16	58	5	35	33	45	95	38%

Given their constant interactions with employees, the help desk serves as the organization's canary in the coal mine: often the first sign of something amiss with, say, the culture in a department or team or with individual behaviors and attitudes or indeed with security is identified as a result of comments to the help desk. It's a wise information security manager who forges strong working relationships with the guys and gals on the help desk. Aside from anything else, they are wonderfully helpful!

We favor the help desk as a single focal point, a call-handling function for all sorts of routine and exceptional communications (e.g., incident reports) with employees on security and other matters, although many organizations have separate contact numbers for IT, HR, site security, IT security, etc. (even though sometimes the calls still end up at the same place!) For the purposes of this example, we have assumed that our hypothetical organization has a small, integrated help-desk function whose main job is to act as a clearing-house, logging all types of calls and coordinating the responses, rather than dealing directly with queries themselves. Like most help desks these days, they log calls routinely through a software application integrated with the phone system, recording details such as the caller's name, the type of call, and the resolving agencies assigned to the case. Naturally, the call logging system has a sophisticated reporting subsystem driving a multitude of displays and generating all manner of fancy reports on things such as call volumes, call waiting times, help-desk statistics, etc.

The imaginary but not unfamiliar scenario that led to us examining {metric 8.9} is that someone (perhaps a security analyst or a security-aware business manager from another function) has come to us excitedly with a bright idea. He or she believes significant changes in the volume of security traffic through the help desk warrant examination by information security as they might signal a malware outbreak or a social engineering attack. Naturally this someone is "far too busy" to sit down with us and actually specify the metric, so we are left making various assumptions about it on our own.

First, we assume that we would in fact be able to persuade the call-logging reporting function to disgorge some form of alert message if the security traffic volume hits a peak. This is generally the easy bit because it is a common requirement, for example, to fire off an alert when certain call conditions are met, such as waiting times approaching or passing a trigger level, meaning the help-desk manager needs to round up the help-desk people loitering out by the coffee machines and persuade them along. Triggering an alert when security call volumes, specifically, hit a trigger level may not be a standard report, but let's assume the system has an ad hoc reporting/alerting function that we can easily configure to our needs. Cool. Because it is fully automated, the **Cost** of the metric will be negligible once it is configured.

Next, we assume the ideal audience/recipient for the metric would be the information security incident manager, who would instantly don his or her bright cape, triumphantly swinging into action, bravely repelling those nasty social engineers, blocking the malware outbreak, or whatever it is.* Unfortunately, however, our putative company doesn't actually have the luxury of a dedicated information security incident manager, so we're a bit stuck here. In practice, the person who would be expected to take charge of such incidents is the information security manager, so he or she is the metric's audience by default. The information security manager is constantly on the go and is not exactly thrilled at the thought of being paged every time security call volumes hit a peak, so we make a mental note to set the trigger point high enough not to go off every few hours.

That brings us to another awkward issue. The information security manager is distinctly cynical, not at all convinced that a surge in security calls is reason enough to fire up the incident response process. The information security manager tells us it is essentially **Meaningless**—any number of situations could cause such a surge in calls, and in fact, they do: a cursory glance at the call-logging system statistics reveals that security call volumes are quite peaky; for example, employees seem to have enormous trouble recalling their passwords every Monday morning. The alerting function could probably be set to ignore Monday morning peaks, but as the information security manager points out, wheedling a password reset from the help desk is a classic social engineering attack. The information security manager is also getting slightly anxious that interrupting an important meeting to investigate *why* security call volumes have gone up is probably not the best use of his or her time. In a nutshell, he or she feels the metric has next to no **Relevance**.

Tip: PRAGMATIC ratings and scores form an agenda, a set of topics to discuss when considering or looking to improve metrics. Remember, this is a decision support tool.

* One of us worked in a place where the head of IT operations, a cheery but physically large and domineering lady, actually *did* wear a bright purple satin cape. You can probably picture her now, swooshing through the department, petrifying the meek cubicle creatures in her path...

At this point, we realize the metric really isn't going to fly. Quickly filling out the rest of the PRAGMATIC table gives us the opportunity to get back to the person that suggested the metric to explain why this particular metric is going to be rejected, given that there are several others that score much higher.

Example Security Metric 8.10

	P	R	A	G	M	A	T	I	C	Score
Culture/worldview	66	30	10	70	40	56	15	40	10	37%

Culture and worldview are intriguing psychological concepts. Cultural theory argues that differing risk perceptions can be explained by reference to four distinct cultural biases (Brenot et al. 1998):

1. *Hierarchists* follow rules and believe in order even when they turn to crime. They intrinsically show respect for the boss and the structure.
2. *Individualists* tend to show little respect for authority: they don't make good soldiers, but it seems they do make good programmers.

Tip: While it is entirely possible that concepts such as this could be developed into fascinating, insightful, and useful security metrics, few of us have the scientific background to do them justice. From a purely practical perspective, most security professionals have more than enough on our plates already without pushing back the frontiers of applied science. Good on you if you do feel inspired to turn theory into practice, developing a novel, scientifically based security metric, but *please* do us a favor before you proudly announce your baby to the security metrics community: use the PRAGMATIC approach to evaluate your suggestion first. Seek second opinions maybe and, ideally, try it to find out how well it works. Look very carefully at every low-rated aspect and figure out if it is feasible to adapt the metric in order to improve its score. If you can honestly get the metric's PRAGMATIC score well into the upper quartile without fooling yourself and without the metric being so narrowly scoped or complex that it is unusable, then go for it! It will be a very welcome addition to our shared metrics catalog. Otherwise, it's back to the drawing board.*

* The higher your metric's PRAGMATIC score, the more attention it will receive from the eager metrics community at www.SecurityMetametrics.com, but please be prepared to explain your metric and defend its high score. It's not that we doubt you or want to discourage innovation—far from it because highly PRAGMATIC security metrics are enormously valuable tools for hard-pressed security managers around the globe. The reason for our cynicism is that we have seen no end of security things that can be measured over the years. The ball is in your court.

Tip: We've said it before, and no doubt, we'll say it again before the book is done: keep notes! It's not too hard to keep a few dozen metrics in our heads, especially the ones we end up using routinely. Bear in mind, though, that business managers and other recipients may not have quite the same interest in or focus on security metrics as us; hence, there is a distinct possibility of them forgetting what certain metrics (especially the ones they only rarely see) are meant to achieve. The net result is that they lose their impact. One outcome we definitely want to avoid is that recipients make something up, completely misinterpreting the metrics. Take the time to explain your metrics, especially the more obscure ones.

3. *Egalitarians* believe authority must be earned and is not an automatic result of position. They can be very effective provided they have charismatic leaders that have earned their respect.
4. *Fatalists*, on the other hand, may obey authority when it suits them but feel it doesn't really matter because we're all doomed anyway!

Depending on which of these quadrants an individual falls into, the theory suggests their behaviors can be predicted with considerable accuracy, and this may have a bearing on risk. Perhaps a metric along these lines would have legs?

Example Security Metric 8.11

Employee turn versus account churn	P	R	A	G	M	A	T	I	C	Score
	30	30	11	36	44	36	62	57	20	36%

Aside from this example metric having a certain lyrical quality to it, its lack-luster score tells us that it probably won't be featuring on many information security dashboards any time soon! The metric is presumably intended to tell us something interesting about the relationships between employees' comings and goings and the number and types of user IDs on our IT systems. Unfortunately, it is far from clear from the cute name what the metric is actually measuring, how, why, and for whom. It's a puzzler.

Example Security Metric 8.12

Organizational dysfunction	P	R	A	G	M	A	T	I	C	Score
	75	20	10	60	80	40	15	10	5	35%

Tip: Cultural assessments and psychometrics are good examples of ways of measuring human behaviors that can generate useful insight for the information security manager, and yet they are seldom used in this field. Don't shy away from these metrics purely because (in your opinion) they appear subjective and indicative rather than objective and definitive. Countering our own bias toward purely technical metrics, remember that human behavior is an extremely important factor in information security. Ignore it at your peril.

Organizations can be dysfunctional in much the same way that some families and individuals are. The manifestations can be very similar. One form of organizational dysfunction leads to a stubborn insistence on doing things the same way, although it consistently fails—a failure to learn and adapt. An easy metric here is the extent of the difference between how the organization sees itself and how others view it: the greater the gap, the greater the dysfunction. This dysfunction is quite common—just read up on Enron or General Motors in its declining years for classic examples. Many other dysfunctions are found in corporate life. Blame culture is a common one, where there is far greater emphasis on finding and chastising a culprit after an incident than on remedying the underlying problems. A blame culture tends to drive incidents underground: naturally enough, employees fear the possibility of personal recrimination if they are blamed for some incident they disclosed even if it was not their fault.

Measuring organizational dysfunctions can range from focusing in on a specific issue, looking for anecdotal evidence to contrast certain functional against dysfunctional situations, right up to broadly scoped organization-wide surveys or assessments by teams of trained psychologists. Keep in mind that a typical corollary of a blame culture is the reluctance or possibly total absence of defined asset ownership. Informal opinions based on anecdotes and casual, nonscientific checks may be cheap, but they are never going to be as reliable or comprehensive as full-on assessments planned and conducted by competent assessors. Transparency, openness, absence of actively concealing issues from audit, or refusing to tackle issues raised by an audit, etc., are indicative of this malady.

Example Security Metric 8.13

	P	R	A	G	M	A	T	I	C	Score
Psychometrics	40	24	0	79	15	55	10	42	5	30%

Psychometric tests, such as OCAI (Cameron and Quinn 1999), MBTI (Myers et al. 1998), or MSCEIT (Mayer et al. 2003) can be used directly as information security metrics or indicators. MBTI, for instance, is a popular scientifically based

approach that categorizes individuals according to four key dimensions of their personality, giving 16 possible MBTI types:

1. *Introverted (I) or extroverted (E)* is about whether you naturally tend to focus your attention inward, within yourself (your inner world of ideas and impressions) or outward, toward the world around you (other people and things).
2. *Sensing (S) or intuitive (N)* concerns the way you take in information either according to what your five senses are presently telling you or using imagination and insight in a forward-looking way.
3. *Thinking (T) or feeling (F)* relates to the way you make decisions based more on rational analysis of the facts or gut feeling.
4. *Judging (J) or perceiving (P)* is about being planned and orderly or spontaneous and flexible.

Using just those four dimensions, someone's MBTI type gives an uncanny insight into their tendencies, likes and dislikes, even the types of career path they are likely to follow and the nature of their personal relationships. Relating the MBTI types to information security would be an interesting exercise: it might be possible, for example, to identify individuals that appear ill-suited to their current roles (which may affect their competence and diligence in performing security activities, such as checking and authorizing important transactions) and perhaps even those with a predisposition toward committing—or indeed discovering and preventing—computer crime or fraud.

Psychometrics may not make the grade as PRAGMATIC security metrics, but they *are* worthwhile tools in particular situations, albeit somewhat beyond the scope of this book.

7.6 Physical Security Examples

Physical access controls underpin information security, given that most other security controls can be undermined, bypassed, or simply broken wide open if an adversary has unfettered physical access to the facilities, IT systems, storage media, and people. Furthermore, physical security protects the provision of essential services,

Tip: Given their intensely personal nature, there are privacy implications to psychometrics. Furthermore, the results need to be interpreted carefully: a tendency, preference, or predisposition for a certain type of behavior is by no means proof that an individual will behave that way in a given situation.

such as power and cooling for the computer suite and, for that matter, food, water, and oxygen for essential employees. This domain also covers alarms—fire alarms, flood alarms, over-temperature alarms, and so forth—plus the procedures for dealing with physical incidents, evacuating the building and securing the assets after the employees have gone.

Measuring physical security has a big advantage over other aspects of security that rely on intangible controls. The strength and other physical properties of a padlock and chain, for example, can be measured using test jigs and strain gauges. The ability of burglars to enter a secure site, building, or room can be tested by simply observing the controls from their perspective and perhaps even trying to force open the doors and windows. Management may be reluctant to sanction the auditors using a chainsaw to cut through wooden doors and walls, a heavy vehicle to ram into the computer suite, guns to threaten the guards, or a bomb to destroy it, but if these are considered serious risks for your data center, it helps if suitable physical controls—meaning proven in tests and in other situations—are built in to the design from scratch. It is wise to reassess the risks and check the controls periodically, implying inspections by facilities maintenance workers, health-and-safety inspectors, and competent auditors.

While many organizations perform logical penetration testing on their IT systems, few in the commercial world undertake physical penetration testing using red teams, tiger teams, or auditors. Given that even strong logical security may be totally undermined or negated by weak physical security, simple prudence suggests that at least rudimentary efforts to gain access to restricted company areas should be attempted periodically. Both of us have personally gained access to supposedly secure buildings using such basic tactics as finding the side or rear door where smokers congregate. After asking for a light and chatting casually to allay any nascent suspicions, building entry is usually straightforward—either the door remains propped open or we simply tailgate in (perhaps struggling awkwardly with a briefcase for a bit of sympathy). Confidently flashing something that vaguely resembles a staff pass has often let us slip past even apparently attentive security guards. People tend not to be suspicious of—in fact, they look right through those who look as if they belong and act right. Busy employees have other things on their mind besides worrying about intruders. One of us once wandered the halls of the Pentagon unaccompanied, even though the visitors badge stated boldly “**ESCORT REQUIRED**.^{*}” Evidently, being well groomed and dressed and walking briskly, appearing purposeful, sufficed not to engender suspicion or comment. In another organization, while waiting to be collected from reception, asking to use the facilities was enough for an unauthenticated visitor to be let through the turnstiles, unaccompanied. Most of us have observed—if not actually exploited—open windows, unlocked doors, low fences, and various other gaps in the perimeter.

* We should say that this was not an attempt at anything nefarious, merely the result of getting lost while seeking the men’s room!

		PRAGMATIC Ratings (%)										
		Predictive	Actionable	Genuine	Meaningful	Accurate	Timely	Independent	Cost	Score		
	<i>Physical and Environmental Security Metric</i>	O	M	S M	M	M	O	O				
9.1	Power consumed by the computer suite versus air conditioning capacity	81	69	92	80	99	98	90	98	88%		
9.2	Physical and environmental security maturity	90	95	70	80	90	85	90	85	86%		
9.3	Discrepancies between physical location and logical access location	75	76	72	90	82	75	85	83	60	78%	
9.4	Number of unsecured access points	95	80	90	70	85	77	45	75	55	75%	
9.5	Number of unacceptable physical risks on premises	70	60	85	60	90	60	30	60	42	62%	
9.6	Distance between employee and visitor parking	1	0	6	93	2	93	66	45	66	41%	
9.7	Percentage of facilities that have adequate external lighting	0	2	5	70	42	11	46	35	18	31	29%

Aside from photographs and notes from physical inspections, many physical controls are (or rather should be) routinely serviced or maintained and tested, for example, checking fire systems to make sure the sensors do actually detect smoke and trigger the correct sequences of alarms and power interlocks. Standby power generators and uninterruptible power supplies are run up on full load every so often to clear the fuel lines, check that they start and run reliably, and confirm that the switchboard wiring continues to power all vital IT equipment if the main supplies fail. There should be records of such tests, which can be used to generate metrics such as time since last fire system check or maximum on-load run time on standby power.

Many physical security systems are instrumented in some way; for example, professionally installed computer room power systems constantly record the supply voltage and current, allowing us to calculate the power consumption. Normally, checking the gauges, printouts, and trends is a routine maintenance or facilities management activity. The individual readings may be too granular for management, but trends, time since last checked/maintained, and other metrics can be very useful yet often overlooked inputs to the information security measurement program.

In the same vein, modern card access control systems, CCTV systems, security guard monitoring systems, and so on tend to be computerized, meaning there are probably useful data recorded on the systems about their operation including security incidents. “Pass card not authorized for this door” events, for instance, are normally logged and may raise the alarm in the case of attempted access to highly secure areas. Unusual patterns or times of access to the computer suite by individual card holders might be cause to investigate what they are up to. Security guards failing to tag all the stops on their overnight rounds could be a sign that they are slacking.

Example Security Metric 9.1

Power consumed by the computer suite versus air conditioning capacity	P	R	A	G	M	A	T	I	C	Score
	81	69	89	92	80	99	98	90	98	88%

It's obvious from the relatively high score that we value this metric! Here's why:

Virtually all of the electrical power supplied to the computer suite or room ends up as heat, a large proportion of which has to be removed by the air-conditioning systems to maintain a stable room temperature. Heat load itself is awkward to monitor, whereas power consumption is quite simple to measure using a suitable clamp-on ammeter on the main power feeds, whether temporarily or permanently fitted. Multiply the rms supply voltage by the total current in amps to calculate the number of watts being supplied.*

* Yes, we know we're ignoring power factor: For our purposes, it really doesn't make much difference, but if your electrical engineers can give you more accurate power consumption figures, so much the better.

Tip: {Metric 9.1} is actually two metrics for the price of one. Power consumption and air-conditioning capacity are two independent variables and could be reported separately, but that would not mean much to management. However, linking them together through this combined metric points out the risk arising from them getting out of alignment. Look out for other similar opportunities with other metrics.

Someone should be measuring and recording the electrical power routinely, periodically comparing it against the air-conditioning system's installed capacity. If the power load increases as a result of installing additional or higher-power equipment (such as high-capacity blade systems in today's dense rack units), the air conditioning has to work harder, placing it under greater stress, and hence, it is more likely to fail. Conversely, if the air conditioning is ridiculously overspecified for the actual load, it may be reliable and have plenty of room for future expansion yet be unnecessarily expensive.

The metric could be of some use for strategic decisions (e.g., planning when to refurbish and upgrade the computer suite) but has more immediate use at the operational level (e.g., if the air conditioners are being pushed hard and summer is approaching, get them serviced now and perhaps arrange some spare/standby portable units and fans for emergency use).

Example Security Metric 9.2

Physical and environmental security maturity	P	R	A	G	M	A	T	I	C	Score
	90	95	70	80	90	85	90	85	90	86%

The way in which the organization manages its physical security, plus the supplies and environmental protection for the computer suite, etc., can be assessed and scored using a maturity scale such as that shown in Appendix H.*

* In our opinion, ISO/IEC 27002:2005 offers useful but rather basic recommendations in the physical and environmental domain, so we have extended it just a little in the maturity metric. For example, the standard's clause 9.1.4 (c), "appropriate firefighting equipment should be provided and suitably placed," is a wonderfully succinct prompt but is hardly the most explicit advice. Who should be providing it? What kinds of equipment are appropriate? Where are these suitable places? Especially given the obvious health and safety implications and likely compliance obligations, we recommend seeking competent professional advice in this area unless you have the particular skills and experience (and even then, get a second opinion!). This book is a practical guide to information security metrics, *not* advice on fire extinguishers, fire alarms, heat/smoke/water detection, power supplies, card access-control systems, antivirus, HR practices, cloud computing, business continuity, backups, privacy, marital breakdowns...

Tip: Someone caught repeatedly committing minor transgressions, such as tailgating, may be demonstrating through their actions a disrespect for the security rules and perhaps dubious personal ethics, which *may* indicate a higher risk of him or her committing more serious incidents, such as theft of proprietary information or fraud. That's a good reason to track incidents of all sorts, gathering and analyzing the metrics for insight.

Example Security Metric 9.3

Discrepancies between physical location and logical access location	P	R	A	G	M	A	T	I	C	Score
	75	76	72	90	82	75	85	83	60	78%

Assuming the organization utilizes some form of automated physical access control system, such as proximity cards to control and monitor/log access to the premises, cross-checking logical access control records against the physical control records may be illuminating. Obviously enough, if a certain employee does not appear to have walked through the access barriers today but logs in to the network locally (a phantom login), there is cause for concern. Is this, in fact, an information security incident? Is someone else using the person's ID? Are they sharing login credentials with colleagues? Have physical or logical credentials been stolen, copied, or fabricated/forged? Have the access controls failed (e.g., an access-controlled door propped open, an unsecured loading ramp left unattended, or a door card reader physically compromised)? Or are employees simply tailgating?*

Comparisons, cross-checks, and reconciliations can be used to generate statistics and, hence, metrics as well as identifying individual issues or potential incidents. Sometimes, as in this case, they raise far more questions than they answer. How many phantom logins are there on average on a normal working day? If we conduct additional security awareness activities on tailgating and authentication, can we reduce the number of phantom logins, and what is a reasonable target reduction over, say, the next six months? Is the number of phantom logins higher or lower on holidays, and why is that?

Example Security Metric 9.4

Number of unsecured access points	P	R	A	G	M	A	T	I	C	Score
	95	80	90	70	85	77	45	75	55	75%

* Tailgating presents an interesting metrics challenge. Card access-control systems that require employees to swipe *out* as well as *in* to a controlled facility ought to be routinely reconciling the respective events: if anyone tailgates, they will probably generate unmatched event records, the daily count of which is, in fact, a tailgating metric. QED.

Tip: It's often possible to milk more value from data-rich metrics in that way, providing summary reports to senior managers with more explicit details for juniors and those who need to address whatever security issues are being identified. Doing so allows the seniors to drill down to the detail if they feel the urge.

It is possible to locate most physical security vulnerabilities through a process of inspection or physical-penetration testing. To do this effectively requires experienced testers who can think like a burglar, knowing the tricks that are commonly used to defeat or bypass physical access controls (such as lock picking, brute force attacks, triggering automatic door lock mechanisms to unlock, insider attacks, gummi fingers for biometric locks, and social engineering). Therefore, the metric has a fair degree of subjectivity. On the other hand, even basic physical security checks tend to identify obvious exposures that clearly ought to be addressed.

Other potential metrics in this area include the following:

- The proportion of attempts that successfully achieved unauthorized access
- The ease with which testers gained access at each attempt*
- How long it took and how many internal areas or sensitive resources could be accessed inappropriately before testers were challenged

{Metric 9.4} could easily be expanded to distinguish and report the different types or relative importance of the physical vulnerabilities identified, provided the additional information would be useful to the recipients.

Example Security Metric 9.5

Number of unacceptable physical risks on premises	P	R	A	G	M	A	T	I	C	Score
	70	60	85	60	90	60	30	60	42	62%

{Metric 9.5} may be a useful way to highlight physical site-security issues, but it is a rather subjective measure unless the unacceptability of risks is defined in sufficient detail. Rather than trying to assess and measure risks, it may be better to measure the effectiveness and efficiency of physical security controls. It is easy

* A Likert item ranging from extremely easy (score 0), quite easy (1), neutral—neither easy nor hard (2), quite hard (3), extremely hard (4), to impossible (5) would make the metric somewhat objective, but a covert video recording from the perspective of the intrusion testers would probably have much more impact with recipients! Is that actually a metric? Who cares? It works! Support for management decisions doesn't *have* to resemble a pie chart.

Tip: {Metric 9.6} is a single example of an entire class of metrics relating to compliance, in this case, concerning physical security control specifications typically laid down in corporate policies and standards. Similar metrics could be developed for every section of ISO/IEC 27002 or every policy in your corporate security manual but have a quick peek at the compliance metrics examples in Section 7.12 for further inspiration in this area.

to spend a small fortune on physical security controls in a glorious but ultimately vain attempt to minimize or eliminate physical incidents, but the law of diminishing returns applies. Control costs can usefully be tracked in categories such as the following:

- Specification and design of physical controls, including periodic reviews and redesign work
- Implementation costs, including procurement and installation/commissioning costs
- Ongoing operational costs, including management overheads, support, routine maintenance, etc.

There is a risk of double-accounting unless care is taken to differentiate physical control measures whose primary purpose is to protect information assets from other physical control protecting fixed assets, etc.*

Example Security Metric 9.6

Distance between employee and visitor parking	P	R	A	G	M	A	T	I	C	Score
	1	0	6	93	2	93	66	45	66	41%

Highly risk-averse organizations that genuinely fear car bombers, ram-raiders, and crack surveillance teams in nondescript white vans bristling with antennas

* Aside from unauthorized or inappropriate physical access, other physical risks include fire, smoke, flood, power failure, dust, sabotage, vandalism, accidental damage, etc., suggesting an entire spectrum of related metrics or possibly some sort of compound metric taking all aspects into account. For instance, working backward from the security end-goal, it is possible to measure and set targets relating to the maximum number of information security incidents with physical causes, for example, the maximum number of fires, floods, or thefts that are expected to occur in the year. The absolute number of incidents is only part of the story, however: their severity is also of concern. If statistics are gathered routinely on the total costs of information security incidents, these may make better targets either in absolute or relative terms (e.g., no individual losses above \$50,000, cumulative losses below \$200,000, or total losses below the level experienced in the previous year).

sometimes arrange separate parking areas to keep visitors further away from vulnerable premises on the presumption that visitors and the general public are more of a risk than employees.* Measuring the separation distance is an example of a simple if rather crude security metric that nevertheless may be of interest, for instance, for management at group HQ to determine whether remote offices take any notice of corporate physical security policies. It is undeniably cheap to measure, although finding someone trustworthy with a long-enough tape measure at every remote office might present a minor logistical challenge.[†]

Example Security Metric 9.7

Percentage of facilities that have adequate external lighting	P	R	A	G	M	A	T	I	C	Score
	2	5	70	42	11	46	35	18	31	29%

Provided ‘adequate’ is reasonably well defined in the form of a set of specifications for external lighting, this is another metric that might be of interest to a corporate/group security function, measuring remote offices through some sort of self-reporting or inspection process. Other physical security controls one could measure with this kind of metric include

- Perimeter security, for example, socioeconomic conditions in the area, suitability and condition of perimeter fences, walls and gates, warning signs, security guard houses, external CCTV coverage and volumetric intruder alarms;
- Internal site physical access security, for example, walls, doors and other barriers, card access controls, locks, on-site CCTV coverage, secure areas, and so forth
- Security guards and receptionists, for example, guard qualifications and experience, number of guards on duty (at all hours), guard rounds (frequency, routes and tracking), etc.
- Essential supplies and environmental controls, for example, deliveries and loading bays, mail, power supplies, air conditioning, fire and flood alarms, intruder alarms, etc.
- Visitor procedures, physical identification and authentication of employees and visitors, lost-card procedures, etc.

* That's quite a presumption in fact!

† This metric potentially has a more subtle purpose, too. Most security controls inevitably get in the way of business. There are real costs associated with, for instance, the frequent delays and frustrations caused to workers moving about any premises that use strict physical access controls, such as card-access systems and turnstiles. Moving visitors further away from the buildings while allowing employees to park closer might even be portrayed as a perk of the job.

Significant differences in the security requirements between sites complicate both the specification of security policies and the measurement of compliance. Physical security requirements or compliance obligations may stem from a number of sources including the following:

- Strategies, policies, procedures, standards, and guidelines generated by the organization and mandated by management (note: facilities, health and safety, human resources, and other functions may impose expectations in addition to information security)
- Laws and regulations imposed by authorities, for example, health and safety legislation and building codes
- Operating conditions specified by the manufacturers of IT equipment (compliance may be optional except that warranty, maintenance, and support arrangements may specify limits)
- Contracts with third parties, such as electricity and telecom suppliers, maintenance services suppliers, other business partners, and perhaps customers or other stakeholders (e.g., physical access controls for government classified materials)

Numeric metrics, such as degree of compliance (expressed maybe as a percentage, a value between 1 and 5, or red/amber/green), may be useful in some circumstances, but the written output of management reviews and compliance audits tend to be much more worthwhile in practice, especially as the implications of noncompliance and potential liabilities can vary markedly according to the nature of the obligations.

7.7 IT Security Metric Examples

Section 10 of ISO/IEC 27002:2005 on communications and operations management actually covers IT security considerations for the ICT network and systems management functions, primarily the IT professionals who lurk within or near the computer suite. Aside from a few recommendations that appear to hint at mainframe-type IT setups, however, the physical type, size, and placement of IT equipment are irrelevant to the security issues raised in Section 10: it applies equally to any IT function, even those with no computer room, not even a computer closet, their IT equipment being distributed on or under desks or carried about nonchalantly by employees in the form of laptops, PDAs, and smartphones.

Although the standard was written years before the advent of cloud computing, a hot IT topic that is still mushrooming as we write, Section 10 does at least include a few security controls for third-party service delivery management, ISO/IEC-speak for IT outsourcing. Cloud computing involves delivering IT services from the cloud, meaning information processing or storage happens on distributed

<i>IT Security Metric</i>	<i>Strategic, Managerial or Operational</i>	<i>PRAGMATIC Ratings (%)</i>							<i>Score</i>	
		<i>Independent</i>			<i>Cost</i>		<i>Timely</i>			
		<i>Accurate</i>			<i>Independent</i>		<i>Meaningful</i>			
		<i>Genuine</i>			<i>Accurate</i>		<i>Genuine</i>			
		<i>Actionable</i>			<i>Genuine</i>		<i>Actionable</i>			
		<i>Relevant</i>			<i>Actionable</i>		<i>Relevant</i>			
		<i>Predictive</i>			<i>Relevant</i>		<i>Predictive</i>			
		<i>S M</i>			<i>M</i>		<i>M</i>			
10.1	IT security maturity	M			S M		M			
10.2	Proportion of systems checked and fully compliant to applicable (technical) security standards	O			O		O			
10.3	Time from change approval to change	M			M		M			
10.4	Correlation between system/configuration logs and authorized change requests	M			M		M			
10.5	Proportion of IT devices not securely configured	O			O		O			
10.6	Rate of change of emergency change requests	M O			M O		M O			
10.7	Proportion of highly privileged/trusted users or functions	M O			M O		M O			

(Continued)

servers located on the Internet or private networks rather than on local servers. Various cloud computing architectures and business models are still developing in this actively evolving area of IT, meaning there are both risks and opportunities.

Arguably, the main concern with cloud computing arises from the organization ceding a large proportion of its control over business systems to third-party cloud service providers. In other words, it has no option but to entrust a significant part of its information security to third parties. Of course, it's not a total abdication of responsibility: there are a number of countermeasures that can and probably should be taken to make sure the suppliers are capable and willing to accept and fulfill their security responsibilities. These are obvious candidates for metrication.

Other important information security controls recommended in Section 10 of the standard include the following:

- Ops procedures, segregation of duties
- Segregation of development, test, and production environments, plus change/configuration management and the promotion of systems on acceptance into production
- Capacity and performance management
- Malware
- Backups and media handling
- Email, eCommerce, etc.*
- Logging and monitoring

Rest assured, we don't intend to offer example metrics for every single control in the standard,[†] just enough to demonstrate the PRAGMATIC approach in context.

Example Security Metric 10.1

	P	R	A	G	M	A	T	I	C	Score
IT security maturity	90	95	70	80	90	85	90	85	90	86%

As usual, we envisage this metric being measured using some sort of maturity scale (see Appendix H, for example).

We hope that by now you appreciate the flexibility and value of the maturity scale approach: scoring criteria can be defined for almost anything, in any level of

* The standard reveals its roots in the 1970s/1980s by using the term “exchange of information” and hinting strongly at electronic data interchange (EDI). The word “Internet” appears just eight times and WiFi not once. Aaah, them was the days, we used to *dream* of being secure...

[†] Supporting the 39 control objectives in ISO/IEC 27002:2005 are 133 clauses (which, confusingly enough, are called “controls” in annex A of ISO/IEC 27001). Those clauses recommend *hundreds* of controls, *thousands* if you count all the obvious variants and derivatives. It is, quite deliberately, an open-ended standard, designed to be applicable to all types and sizes of organization and addressing an enormous range of information security risks.

detail, by someone who has sufficient experience to recognize the range of possible options. It took us just a few hours (well, OK, a couple of days) to prepare Appendix H from scratch using ISO/IEC 27002 for inspiration on both the structure and the specific controls.

Example Security Metric 10.2

Proportions of systems checked and fully compliant to applicable (technical) security standards	P	R	A	G	M	A	T	I	C	Score
	81	77	89	86	89	73	74	78	70	80%

Here, we measure the technical security compliance processes and activities* using a pair of distinct but closely related measurements:

1. First, we measure what proportion of IT systems are compliance-checked against technical security standards. The standards may be purpose-written for corporate use or public standards (such as various security baselines offered by vendors, such as HP, Sun, and Microsoft, or by bodies, such as the Center for Internet Security or the Information Security Forum) or customized corporate versions of the latter blending both approaches. The metric effectively differentiates those parts of the IT landscape that have been compliance-checked (to an adequate level) from those that have not. It is both a measure of the compliance effort and a prerequisite for the accompanying metric. The reality is that 100% compliance testing is only very rarely possible let alone worthwhile. Furthermore, compliance tests tend to combine actual hands-on tests of systems sampled from the population with other, more-cursory checks, projections, and assumptions. Automated compliance checking is often possible for at least some of the security configurations and parameters.
2. Second, homing in on the systems that have, in fact, been adequately compliance-checked, we determine the proportion of systems that have been confirmed compliant with the standards. This obviously reflects the implementation and management of security on those systems.

The net result of {metric 10.2} is management information concerning the quality of technical compliance-checking and the technical security status of the systems—in other words, this is an information-rich metric that is particularly suited to those making operational decisions about security. The numbers would take a lot of explaining to senior management but can be used more or less immediately by security analysts and operations professionals to work on improving technical compliance-checking and technical compliance.

* This could equally have been classified as a compliance metric.

Tip: The conundrum raised by this kind of metric can be addressed by (1) setting an ideal/target time for the metric that is not zero but allows all the essential pre-implementation steps to be completed; (2) measuring the *effectiveness* as well as the *efficiency* of the process because these are complementary aspects; and (3) separating ordinary from emergency changes, applying different ideals/targets for both, perhaps even separate metrics.

Example Security Metric 10.3

Time from change approval to change	P	R	A	G	M	A	T	I	C	Score
	70	71	76	90	60	84	64	60	80	73%

For various reasons,* we haven't offered many examples of security process metrics, but here's one, in effect measuring the efficiency of the (IT) change approval/implementation activities. Approval implies that some form of risk evaluation and the change authorization process takes place prior to implementation, which, in turn, implies delays when implementing changes that are likely to be beneficial (such as security patches). Speeding up the implementation of security patches would seem to be *a good idea* because it reduces the exposure window in which the security vulnerabilities (we hope!) addressed by the patches are more likely to be exploited. At the same time, however, the possibility of rushing the pre-implementation risk assessment, testing, and authorization activities increases the risk that inappropriate changes will be hurriedly made, perhaps making this a double-edged metric.

Example Security Metric 10.4

Correlation between system or configuration logs and authorized change requests	P	R	A	G	M	A	T	I	C	Score
	87	80	90	80	80	80	60	50	47	73%

{Metric 10.4} is a process compliance metric in the context of IT change management. Simply stated, unauthorized changes to IT systems probably qualify as information security incidents.

The metric is quite strong but suffers a little on the Independence criterion because it is quite likely that the people correlating log records against change requests would be involved in the change process, so they would have a direct interest in the outcome. They might just be tempted to err on the side of achieving their

* The primary reason is that we are generally more interested in achieving positive security outcomes for the business than in the processes and effort required to get there. We don't always have the luxury of that choice.

Tip: We have more to say on validating important metrics in Chapter 9, but for now, note that neither the measurement nor the validation need necessarily be routine or continuous activities. Correlation or reconciliation-type checks and the associated metrics can often be performed on a sample basis with the caveat that if significant discrepancies are found, follow-ups plus more frequent or elaborate checks may be justified.

annual bonus rather than diligently reporting every single discrepancy they find. Luckily, the data they are analyzing should be subject to change and access controls and could potentially be cross-checked by someone else if there is some reason to doubt the metric's integrity or validity. Having one or more technical people cross-match log entries against change requests is perhaps not the best use of such valuable resources, which also affects the **Cost** rating.

Example Security Metric 10.5

Proportion of IT devices not securely configured	P	R	A	G	M	A	T	I	C	Score
	83	80	77	75	59	74	76	88	36	72%

Wouldn't it be great to have a number like this! There are, however, issues with it in practice.

First, there's the question about what is meant by "securely configured." Elsewhere, we discuss a compliance example {metric 15.8} comparing actual security configurations against security standards: here, we are potentially talking about bespoke configurations that may or may not address the security requirements on a specific IT system, regardless of security standards.

Second is the effort involved in measuring the security configurations. We may be lucky enough to have automated configuration-checking tools running on all

Tip: Phrase security metrics in a positive way wherever possible, such that improvement is indicated by the numbers going up: 100% should always mean a top score with 0% being abject failure.* More than that, try to avoid negative language or words with overtly negative connotations if you can. This goes beyond mere spin. Done well, information security supports and enables the business. Say so!

* On this basis, some might quarrel with our use of **Cost** as the last of the PRAGMATIC criteria because 100% actually means low cost. We are a little hamstrung by the PRAGMATIC mnemonic, but if it makes you feel better, by all means take the C to mean **Cheap**. We chose not to do this because the criterion is actually about cost-effectiveness and value, not cheapness, which smacks of cheap-'n'-nasty or shoddiness, the antithesis of what we are about.

our systems or the resources to check them manually, but either way, that involves a lot of time, effort, and expense. Is the metric really worth it?

Third, what would the proportion of IT systems figure really tell us? Suppose this metric sat at 50%, meaning half our IT systems were not securely configured. Does that necessarily mean the remaining 50% definitely were securely configured, or is it just that we hadn't checked them all yet? If the metric went up to, say, 75%, that would mean things had gotten worse. This is an example of a metric that is at once both confusing and depressing!

Example Security Metric 10.6

Rate of change of emergency change requests	P	R	A	G	M	A	T	I	C	Score
	64	71	69	73	78	70	70	69	83	72%

Emergency change requests are those that get forced through the normal change review, approval, and implementation process to satisfy some urgent change requirement, shortcircuiting or even totally bypassing some of the steps in the conventional process. Often the paperwork and management authorization is done retroactively. Emergency changes are inherently risky but are often treated as a necessary evil, particularly when the conventional process is glacially slow in comparison to the rate of change needed by IT and the business.

The metric is slightly weak on Predictability because there are many factors involved, not just security.

Example Security Metric 10.7

Proportion of highly privileged/trusted users or functions	P	R	A	G	M	A	T	I	C	Score
	86	80	51	40	65	39	55	95	60	63%

{Metric 10.7} is indicative of the organization's ability to control privileged access. From time to time, we have performed the checks necessary to gather and analyze the raw data for this metric with fascinating results. We have seen systems where *every single* user ID has full administrative rights "because it was convenient to do it that way." We've found very similar systems in the same company with dramatically different proportions of privileged versus nonprivileged accounts as a result of serious discrepancies in the account authorization and security administration processes used by different departments. It is so commonplace to find that long-term IT professionals have accumulated every privilege in the book* that we smell a rat if we *don't* find this!

* Along with having so many accounts on so many systems that they are not at all certain whether there are any systems they *can't* access. And if you find this, by the way, check how they recall all those passwords.

Tip: In the right hands, system security/audit tools turn what is otherwise a mind-numbingly tedious activity to gather and analyze the data into a delightful voyage of discovery revealing new horrors around every corner. Once again, availability of data is not the issue: the real challenge with this metric lies in framing and posing the appropriate questions and, of course, dealing with the findings and the fallout.

The metric could be a very granular and rich source of information provided someone has the time, energy, and integrity to analyze and report against them. It's a good metric for IT auditors.

Example Security Metric 10.8

Entropy of encrypted content	P	R	A	G	M	A	T	I	C	Score
	78	66	23	78	3	93	74	79	34	59%

Randomness is *a big deal* in cryptography. Strong encryption algorithms generate output that is as close to random as can be. A well-encrypted stream of data superimposed on top of white noise would appear to an observer to be just white noise—there should be no discernible hint of the presence of encrypted information (in fact, that is not a bad description of steganography). The so-called “one-time pad,” the only provably 100% secure method of cryptography, is absolutely dependent on the randomness of a key at least as long as the data to be encrypted.*

Conversely, patterns are like gold dust to a cryptanalyst trying to locate or reconstruct the original information from encrypted data. Even the vaguest hint of repeats or nonrandom sequences may give the cryptanalyst sufficient clues or cribs to break the code.

OK, that's all very well in theory, but let's consider it in a more practical everyday setting. Imagine being faced with a bunch of security products that all claim to use the latest high-tech encryption techniques and ridiculously long keys. How can you verify that the outputs are, in fact, strongly encrypted? You could compare the products in terms of the algorithms and the number of bits in the keys, but what if (shock! horror!) the vendors are lying or have made genuine mistakes in how their products are constructed?

You might perhaps take a good look at the source code for the encryption modules, assuming you know what you are looking at and assuming that you are truly able to examine the source code for the encryption functions in the products of

* Despite the name, the one-time pad must be used precisely twice: once to encode, once to decode. Two-times pad would be more accurate.

interest.* Alternatively, you could try cryptanalyzing the output, perhaps using known plaintext to make your job just a little easier. But what if you are not a competent cryptanalyst with the time and skills to do the analysis or with the vast resources to outsource the task to specialists?

Measuring the strength of cryptographic systems is a tough challenge yet a very important one for those of us who are heavily reliant on keeping vital data confidential through encryption. {Metric 10.8} takes a markedly different approach, directly measuring the randomness or entropy of encrypted data. The actual measurement process is pretty straightforward in theory: simply obtain a very large quantity of encrypted content and run it through a utility that searches for patterns and nonrandom distributions of the bits, generating statistical data to indicate the degree of randomness or predictability. It would take rather more effort to figure out exactly *how* random the data need to be to satisfy a given security requirement, but already our metric offers an easy comparator between encryption products.

The fact that this metric concerns cryptography, technology, mathematics, *and* extreme risks and has taken us half a page to explain to you is the reason for its very low rating on Meaningfulness. That aside, it is an intriguing metric.

Example Security Metric 10.9

Percentage of IT/ process changes abandoned, backed out, or failed for information security reasons	P	R	A	G	M	A	T	I	C	Score
	50	70	55	60	65	40	50	45	60	55%

{Metric 10.9} is another measuring procedural deficiency. The precept here is that IT or business process changes that eventually ended up being abandoned or reversed out or that failed in service creating incidents should ideally have been blocked *prior* to implementation by the change testing and authorization processes; hence, they indicate failures, weaknesses, or gaps in those very procedures.[†]

* Whether you are deemed completely paranoid or just sensibly cautious if you *insist* on compiling cryptographic functions from the source code using your own trusted compilers and systems depends on the context. This level of risk aversion is not unheard of in national security work for good reason.

[†] This could turn out to be a really unhelpful metric if it ends up driving the process too hard toward security and excessive risk aversion to the extent that changes that are *desperately* needed by the business but are even remotely risky get blocked or unduly delayed. The fact is that although every change creates risk, not changing can also be risky. Paradoxically enough, extreme risk aversion is reckless, career-limiting for sure.

Tip: Unlikely as it may seem, there are some well-structured ways of assessing and categorizing vulnerabilities; therefore, simple counts of the number of vulnerabilities in each category would give a rough and ready measure of technical vulnerability with just enough detail to be really interesting.*

* See OSVDB for example. Alternatively, develop your very own vulnerability categories: it's not hard at first.

Example Security Metric 10.10

	P	R	A	G	M	A	T	I	C	Score
Vulnerability index	74	85	71	74	60	32	46	33	19	55%

In the specific context of IT security metrics, “vulnerability index” implies some sort of automated scanning/identification, scoring, and ranking mechanism for technical vulnerabilities discovered on the IT systems, although, strictly speaking, it might also cover nontechnical vulnerabilities within IT.*

There are definitely issues with the Accuracy and scope of the automated vulnerability assessment tools, and the good ones are hardly low-Cost, but on the whole, we are much better off with them than without them.†

Example Security Metric 10.11

	P	R	A	G	M	A	T	I	C	Score
Delays and inconsistencies in patching	43	41	77	62	36	32	48	34	42	46%

Although—regrettably—patching vulnerable operating systems and applications is an essential part of IT security, there are often reasons for delaying patching,

* A broad-based vulnerability or risk index for cloud computing applications/systems has a certain attraction, encompassing not just technical issues but the service, relationship, privacy, and ownership aspects, too. Furthermore, we are keen to see cloud customers start demanding and cloud suppliers start supplying PRAGMATIC security metrics—measures that are **Predictive** (forward-looking, proactive), **Relevant** (to security, compliance, and to the commercial relationship), **Actionable** (not just “Last quarter’s uptime figures were...” Please!), **Genuine** (credible, verifiable, auditible even), **Meaningful**, **Accurate**, **Timely**, **Independent**, and **Cheap** (worthwhile for *both* parties).

† Just don’t say or imply or give even the vaguest, merest, slightest whiff of a hint that a clean bill of health from \$chosen-vuln-scanning-tool means anything other than “*We haven’t—yet—found all the technical vulnerabilities in this system.*” Seriously, be careful, be scrupulous, print it out poster-sized and put it on the wall above your desk if you like. Certain managers still won’t *get it*, but at least now it is *their* problem, not yours.

Tip: Given that prompt and efficient patching is such a vital information security control in these days of ubiquitous Internet connectivity, this measure could certainly be classed as a KRI.*

* However, the poor PRAGMATIC score for our example metric leaves plenty of latitude for you to come up with improvements!

such as to check whether urgent/critical security patches might break critical applications.* The fact remains that there should be slick procedures for performing this routine security maintenance activity as efficiently as possible. Time is of the essence.

We slipped a small but important extra consideration into the example metric: the notion that patching should be consistent. We are hinting at the need to patch all vulnerable systems, not just the most obvious and immediately accessible ones. It is noticeable how often hackers are able to establish beachheads inside organizations by exploiting systems that remain vulnerable and unpatched as a result of being a bit off the beaten track—test systems, portables, and even systems used for systems/network administration, for instance.[†]

Patching procedures, or rather the risk assessment aspects, should take into account the risk of *failing* to patch and should preferably incorporate compensatory controls when that risk becomes unacceptable and emergency patches are pushed through the system.

Example Security Metric 10.12

Perceptions of rate of change in IT	P	R	A	G	M	A	T	I	C	Score
	40	50	6	65	70	50	30	14	40	41%

Because it involves perceptions, {metric 10.12} is patently a highly subjective measure that limits its absolute Accuracy and Independence ratings. However, extreme values (meaning the rate of change is perceived as being far too fast—or indeed far too slow) suggest there are increased information security risks compared to a situation in which changes are happening at a more reasonable rate.

* We know of a bank that was very nearly brought to its knees by such a patch: if the emergency patch rollout had gone ahead without adequate testing, the online banking applications would have gone offline, perhaps for several days, while the resultant mess of spaghetti was carefully un-knitted. Chalk that one up as another win for security!

[†] This illustrates a fundamental inequality of information security: the white hats have to defend every single inch of the castle walls, while the black hats only need to find one tiny weak point in the portcullis—although admittedly they do also need to dodge the boiling tar. And the volleys of flaming arrows. Oh, and the trebuchets.

Tip (an *extremely* simple tip this one): Use italics or bold face or color to emphasize key words in the metric if it reduces ambiguity, but do so sparingly or it loses its impact.

Similarly, sudden changes in this metric indicate that *something* is going on, which again *may* have a bearing on information security.

Aside from the metric being no help whatsoever in terms of what we are actually expected to do if it indicates trouble (a very low Actionability rating), it is hard to establish much of a relationship to security.

Example Security Metric 10.13

Patching policy compliance	P	R	A	G	M	A	T	I	C	Score
	66	52	55	77	19	36	11	8	5	37%

If the organization has a set of policies and procedures for patching, the level of compliance is of significance and perhaps reflective of overall policy compliance in the organization. However, the metric doesn't score well mainly because it is not likely to be **Timely**, is cumbersome (**Costly**) to monitor, and is measured by people with a direct interest in the subject areas (not **Independent**).

Example Security Metric 10.14

Number of changes	P	R	A	G	M	A	T	I	C	Score
	55	24	9	6	2	3	15	26	67	23%

Changes invariably affect the risk level; therefore, this metric has some merit because it is easy and **Cheap** to measure. The low score results mainly from a lack of **Meaningfulness** and **Accuracy** insofar as it is very context-dependent, for example, implementing a new system or application will result in many changes that may, in fact, serve to *reduce* risk.

Tip: You will have noticed that we have numbered our example metrics according to the sections of ISO/IEC 27002:2005 and the ranked scores in each section. You are free to adopt whatever identification scheme you like—the point is to have one and stick to it as it makes it easier to refer to your metrics when reviewing and using them. You might, for example, incorporate the year the metric was first used in the organization as a reminder that new metrics mean new issues to consider.

Example Security Metric 10.15

Number of viruses detected in user files	P	R	A	G	M	A	T	I	C	Score
	8	13	6	11	3	2	5	5	78	15%

We may scoff at metrics such as this, but, sadly, there are undoubtedly misguided organizations using them. Actually, that's a bit unfair because there may conceivably be particular circumstances in which someone genuinely needs to keep tabs on how many viruses have been detected in user files or some such arcane metric. In the context of our imaginary organization, however, the dreadful score for this metric knocks it out of the game without much more ado.

Example Security Metric 10.16

Number of firewall rules changed	P	R	A	G	M	A	T	I	C	Score
	2	1	1	10	2	33	14	4	17	9%

Having read this far, it should come as no surprise to you that this metric scores abysmally. It doesn't even reach double digits on five out of the nine PRAGMATIC criteria. This is another very context-dependent metric that depends heavily on what's going on in the organization. If we know enough about the situation to understand the metric, the metric itself tells us nothing more.

Example Security Metric 10.17

Toxicity rate of customer data	P	R	A	G	M	A	T	I	C	Score
	0	0	0	0	0	0	0	0	0	0%

We are including {metric 10.17} as an extremely bizarre example—so bizarre and so extreme, in fact, that we honestly don't have a clue what it is meant to be measuring nor why one would have the slightest interest in it. Metrics of this nature do crop up from time to time; in fact, this is based on a genuine example that we vaguely recall having seen discussed, somewhere.

Anyone familiar with those horrendous corporate value objectives, visions, and mission statements should recognize the symptoms of excessive wordsmithing. Our guess is that at some point, someone has probably been reporting a particular metric relating to the integrity of customer data, which is ostensibly a perfectly reasonable thing to measure. The metric as originally worded may not have worked out for whatever reason, so it was reconsidered, altered somewhat, and the wording modified accordingly, probably by committee. Lather, rinse, repeat a few times, and pretty soon, we end up with the kind of obscure language used in this example. The specific words used are, no doubt, heavily laden, dripping with significance. It may still mean something to the managers and practitioners who originally discussed it at length in fraught

	Access Control/Metric	PRAGMATIC Ratings (%)						Score				
		Independent	Cost	Timely	Accurate	Meaningful	Genuine					
11.1	Rate of messages received at central access logging/alerting system	O	87	88	94	93	93	94	97	89	79	90%
11.2	Information access control maturity	S M	90	95	70	80	90	80	90	85	90	86%
11.3	Days since logical access control matrices for application systems were last reviewed	M O	55	80	95	30	80	85	60	70	80	71%
11.4	Proportion of inactive user accounts that have been disabled in accordance with policy	M O	68	56	74	76	73	64	64	52	75	67%
11.5	Rate of detection of access anomalies	O	83	86	65	75	70	52	44	61	11	61%
11.6	Logical access control matrices for applications: <i>coverage and detail</i>	M O	60	70	65	70	78	68	50	50	20	59%
11.7	Logical access control matrices for application systems: <i>state of development</i>	M O	70	50	60	60	88	25	40	20	40	50%
11.8	Quality of identification and authentication controls	M	60	87	40	40	56	36	41	22	42	47%
11.9	Proportion of business units that have <i>proven</i> their identification and authentication mechanisms	M	69	73	72	32	36	4	56	2	50	44%
11.10	Number of times assets were accessed without authentication or validation	O	61	78	33	16	33	0	44	35	33	37%

Tip: If your internal corporate metrics are formally documented at great length in explicit detail using very precisely defined terminology, often on rather tedious and boring forms, *you may just be completely missing the point*. There *are* valid situations in which that level of precision may be appropriate or necessary (e.g., security metrics used as part of the legally binding contractual specification for, say, a cloud-computing service), but the most useful information security metrics are elegant in their simplicity. It shouldn't take a PhD to understand what a metric says or means. Within reason, less is more.

meetings. To anyone not privy to the inside track, however, or to those who have long since forgotten the arguments, it is pure gibberish. It might as well be in hieroglyphics.

7.8 Access Control Example Metrics

Access controls fall roughly into two categories: physical and logical. We have already described a few physical access control metrics in Section 7.6, so now we concentrate on logical access controls. Logical security involves important technical information security controls, such as data, system, and network access controls (including encryption); access rights, roles, and privileges; identification and authorization; and management, including assignation, configuration, and review of access rights, etc.

Example Security Metric 11.1

Rate of messages received at central access logging/alerting system	P	R	A	G	M	A	T	I	C	Score
	87	88	94	93	93	94	97	89	79	90%

The rate at which access-related events are received from a variety of distributed systems by a centralized access management, logging, and alerting system scores surprisingly well against the PRAGMATIC criteria. It turns out that the rate not only gives useful information about possible access control issues but also acts as a heartbeat for the access control system as a whole.

First, think about the distributed systems. Access control events tick along at a steady rate on all the systems, but suddenly there's a rash of events on one system. What could it be? Straightaway, we have a possible incident in progress. We know which system has the issue, when it happened, and we know from the messages what kind of incident it is. At this stage, if we are quick, there is a reasonable chance we can deal with the situation before it causes any impact. If it turns out to be a simple explanation (maybe an automated system that is failing to connect or a user trying a bunch of passwords because he or she has forgotten his or her own), we can

probably resolve it in minutes and, in the process, make it clear that we are watching the logs—which sends a powerful awareness message in its own right.

Now imagine the situation where, instead of seeing events tick along as normal, we notice an unusual dip. Looking at the data, we see that a system or a bunch of related systems appear to have had no events for a while when normally we would expect a steady stream. Again, we know which systems to investigate further, we probably know when the anomaly started, and we are on top of it promptly.

The rating is slightly down for **Predictability** because the events that we see or don't see have already passed, but we may be watching a determined hack or some such incident unfold before us or about to happen (e.g., when an automated password guesser finally hits pay dirt). **Relevance** takes a slight hit because we could be dealing with simple network, system, or user issues with relatively minor security implications.

The lowest rating for **Cost** is because of the effort required to set up not just centralized reporting/access control (which has many other benefits) but also the metric reporting and alerting. Clearly, it will take some effort to monitor and respond to issues, but we feel there are substantial benefits to this metric.

Example Security Metric 11.2

Information access control maturity	<i>P</i>	<i>R</i>	<i>A</i>	<i>G</i>	<i>M</i>	<i>A</i>	<i>T</i>	<i>I</i>	<i>C</i>	<i>Score</i>
	90	95	70	80	90	80	90	85	90	86%

Yet another maturity scoring scale is provided in Appendix H.

Example Security Metric 11.3

Days since logical access control matrices for application systems were last reviewed	<i>P</i>	<i>R</i>	<i>A</i>	<i>G</i>	<i>M</i>	<i>A</i>	<i>T</i>	<i>I</i>	<i>C</i>	<i>Score</i>
	55	80	95	30	80	85	60	70	80	71%

This per-system metric indicates the effectiveness of the processes through which access rights are being monitored and maintained. The metric scores strongly in terms of being **Actionable**: it is obvious that if the metric is too low, it is time for the matrices to be reviewed. In practice, using this kind of metric would probably involve setting targets for the appropriate review periods for various classes or

Tip: The maturity scoring scales are eminently flexible and adaptable. Seen some factor that isn't already taken into account? Just add it in. Noticed a substantial advance in the state of the art—perhaps a new form of control? Adapt the marker texts accordingly. Want an even higher-level overview metric? Combine or simplify some of the rows.

types of systems and measuring discrepancies between actual and target dates in days: some matrices will have been reviewed on or before their targets; others will be overdue. We presume the raw data—target and actual dates—may be read from some sort of inventory of the systems, populated in turn from the access matrix review and update procedures. This metric also scores highly in terms of Accuracy, given the number of days between target and actual dates are readily measured and checked, although there is still a practical question of determining the date an access matrix is declared fully reviewed. It is quite conceivable that this date might be deliberately manipulated by someone seeking to improve his or her score, so the metric is rated down on Genuineness.

Example Security Metric 11.4

Proportion of inactive user accounts that have been disabled in accordance with policy	P	R	A	G	M	A	T	I	C	Score
	68	56	74	76	73	64	64	52	75	67%

Timely measures of compliance are useful, and this is a fairly straightforward measure to achieve that objective. Comparing data from HR against account status is simple. It could be classed as Security 101. Disabling computer accounts when people move on is such a basic control that if it is not being performed well, chances are there are probably far more serious issues with the user administration processes.

Example Security Metric 11.5

Rate of detection of access anomalies	P	R	A	G	M	A	T	I	C	Score
	83	86	65	75	70	52	44	61	11	61%

With access control being the first line of defense, the ability to detect access anomalies ranks pretty high in maintaining adequate security. This metric is similar in intent to {metric 11.1} but is missing the centralized control/reporting element. We assume it might involve someone manually checking a number of systems for anomalies, which is a tedious and costly process compared to the automated, centralized approach.

Example Security Metric 11.6

Logical access control matrices for applications: <i>coverage and detail</i>	P	R	A	G	M	A	T	I	C	Score
	60	70	65	70	78	68	50	50	20	59%

The concept behind {metric 11.6} is perfectly sound: someone should, from time to time, check that application access control matrices or entitlements (specifying the access rights for roles to data and functions) are reasonably up to date, that is, they are, in fact, being used. If not maintained, they can rapidly decay until they are no longer of any use, by which time it is highly likely that access rights on the systems are in a complete mess.

Example Security Metric 11.7

Logical access control matrices for application systems: <i>state of development</i>	P	R	A	G	M	A	T	I	C	Score
	70	50	60	60	88	25	40	20	40	50%

This metric aims to highlight systems that are probably lacking in effective access controls because of their primitive state of development. Despite our obvious liking for maturity-scale metrics, it is not entirely obvious how we might define maturity criteria for the development of access controls, rendering that approach inappropriate here.* Suppose we try a different route, perhaps asking the application development and support teams to self-rate their use of logical access control matrices.

Straightaway, we have given ourselves a serious problem in that the people providing the data for the metric obviously have a vested interest in the subject matter. Nobody likes to admit they are doing badly at anything, especially with respect to things relating to their chosen profession. It's a matter of professional pride. The tendency is to rate his or her own performance way above reality.[†] As a consequence of the low Independence factor, the Accuracy rating is also depressed, giving a poor overall score for the metric (especially considering the maturity-scale metrics have been scoring in the high 80s).

Tip: Coverage and detail-type metrics can be used to contrast good against bad examples and prompt good practice sharing as well as simply scoring them.

* We're being a bit hard on ourselves. With some research and thinking time, we probably could figure out a meaningful set of maturity criteria, but let's assume—for the sake of argument—that we're not happy with the result, so we need to think about other ways of measuring it.

[†] A number of the observer biases outlined in Appendix J could be relevant here. We're conscious, also, that in claiming the application teams are likely to offer biased self-assessment scores, we are implying that *we* would score them more objectively because we are independent, revealing our own observer bias! Are we even competent to assess the development of access control matrices? It's by no means certain that we would score them any more accurately than they would score themselves.

Tip: Controls that aren't nurtured and cared for tend to decay over time. Keeping an eye on important controls through metrics is one way to ensure they are not neglected.

Example Security Metric 11.8

Quality of identification and authentication controls	P	R	A	G	M	A	T	I	C	Score
	60	87	40	40	56	36	41	22	42	47%

While the quality of identification and authentication controls (i.e., their fitness for purpose) is vitally important, the metric scores quite badly primarily because of its lack of Independence, Accuracy, and Genuineness/objectivity. Who determines the quality ratings and how? The metric name is very vague, making it hard to determine how well it would function. With a bit more work on the specification, this could turn out to be a far more valuable metric, especially given that identification and authentication are such important information security controls.

Example Security Metric 11.9

Proportion of business units that have proven their identification and authentication mechanisms	P	R	A	G	M	A	T	I	C	Score
	69	73	72	32	36	4	56	2	50	44%

Validating or proving identification/authentication/identity management controls gives an indication of their quality. However, there are many different ways of achieving that, ranging from audits or tests by competent, trustworthy, and independent assessors against detailed specifications down to rough-and-ready self-assessments. Because we cannot determine the details from the short metric title alone, we gave the metric extremely low ratings on Accuracy and Independence.*

Example Security Metric 11.10

Number of times that assets were accessed without authentication or validation	P	R	A	G	M	A	T	I	C	Score
	61	78	33	16	33	0	44	35	33	37%

* In practice, we would anticipate having rather more information on each metric, such as completed standardized metric specification forms. Furthermore, it is worth identifying, considering, and clarifying important details in the course of the PRAGMATIC rating/scoring process, retaining notes, and perhaps updating those specification forms accordingly.

If only it were feasible to measure this in a scientific, objective manner! One of the inherent problems with access controls, particularly identification and authentication, is that if they fail, we are unlikely to know about it, at least not at the time. If a hacker somehow succeeds in fooling a computer into believing he or she is someone else, perhaps by stealing that person's logon ID and credentials, the computer will go along with the ruse unknowingly, as it were, for an indefinite period. Likewise, if a social engineer obtains an authentic-looking ID badge, he or she may be able to come and go from the building at will, gaining more confidence and credibility every time he or she passes the security guard or receptionist.

7.9 Software Security Example Metrics

ISO/IEC 27002:2005 Section 12, "Information Systems Acquisition, Development, and Maintenance," briefly covers extremely important IT controls relating to the development and implementation of software application systems, including the following:

- Definition of security requirements (alongside business requirements)
- Validation of data entry, processing, and output, plus message integrity
- Cryptography (only covered at a high level—policy and key management)
- Control of system files, test data,* and source code
- Security aspects of the software development process
- Technical vulnerability management

Change and configuration management (including control of operational software and change control procedures covered separately in the ISO/IEC standard) have information security implications that extend far beyond software development, for example, changes to the following:

- The business processes and activities supported by IT application systems
- Information security risks, for example, different threats, vulnerabilities, impacts, attack modes, etc.
- Personnel including employees; pseudo-employees, such as temps, contractors, and consultants; and nonemployees, such as advisors, regulators, and competitors

* Aside from suggesting that test data should be protected (primarily for privacy reasons, which implies that it is OK to use personal data for testing purposes), ISO/IEC 27002:2005 is not exactly forthcoming on the need for security testing, nor does it have much to say about security activities that should be associated with or integrated into software development activities.

Change management has important ramifications on information security for several reasons, the main issue being that information security threats and vulnerabilities, plus information technologies and business processes, are all inherently dynamic. Many of the security controls that were generally appropriate and sufficient in the past may no longer be adequate because many of the threats, vulnerabilities, and impacts of incidents are different today.*

Managing changes well is generally a sign of an organization that has things under control as opposed to those that don't have a firm grip on things and are thus at the mercy of changes caused by or imposed on them, some of which may well be inappropriate and unwelcome. Even worse in some ways, organizations that aren't good at change management can miss out on business and improvement opportunities that arise, either because they fail to appreciate the possibilities or fail to respond to and exploit them effectively.

Change management involves the following:

- Identifying, assessing, and, if necessary, responding to changes that occur, whether or not they are intended, managed, or appropriate
- Also identifying the need or impetus to change, for example, the possibility of taking advantage of new opportunities
- Assessing possible changes to determine which, if any, are appropriate and don't pose an unacceptable risk
- Planning and preparing for changes, for example, specifying the key parameters and goals and lining up the necessary resources
- Making appropriate, intended changes in a controlled manner
- Monitoring and measuring the change process and changes made to determine whether goals are met, adapting the process as necessary to stay on track

Change processes may already generate or could be modified to collect, suitable metrics. The \$6 million question, of course, is what do we mean by "suitable metrics"?

Take the typical software development projects, for example. Software development is often an integral part of major business changes and, as a process, is often reasonably well structured and controlled. Issues such as test failures, implementation issues/incidents, and post-implementation support problems all speak to the quality of the development process. Simply collecting and tracking the raw numbers across different projects helps management get a grip on how best to manage projects, and most organizations that do in-house development have some form of quality assurance monitoring in place.

* Notice we said "most" and not "all." The so-called 419 advance-fee scams, for example, that now arrive almost entirely by email used to be distributed by airmail letters, telexes, and faxes. Cheap electronic distribution means they reach many more of us than in years gone by, but the hooks and psychological tricks used to defraud victims are practically identical—as indeed are the poor grammar and dodgy spelling!

Process controls for the software development process may not be tracked, however, because failures typically indicate compliance issues that those involved in such projects are seldom keen to disclose. Process controls in this context include the following:

- Stage gates or management decision points between major phases of the project, where prior activities are supposed to generate sufficient, reliable information for managers to make rational decisions, and various access and other controls prevent the project from bypassing or overruling such management decisions.
- Resource management is tracked through budgets and expenditure figures for the project's finances and human resources. The typical project management office is usually awash with numbers to analyze, perhaps with help from finance or the HR department.

Finally, most change projects start off by building business cases that project the costs and benefits in sufficient detail for management to approve, modify, or disapprove the necessary investment. Well-managed projects maintain their business cases throughout the development and implementation phases, right through into production. They monitor the process to ensure the project is consistent with the original assumptions, for instance, checking that expenditures remain within projected bounds, all the while firming up the projected business benefits. At implementation time, the benefits should be as concrete as they will ever be, forming an ideal set of metrics to demonstrate the value of the change.

Configuration management is a subset of change management concerning the management of configuration changes to technologies, particularly IT systems, in this context.

Quality has been studied, developed, and applied over many decades but, curiously enough, is rarely considered in relation to information security. Particularly in the period since World War II, quality assurance (QA), total quality management (TQM), and related disciplines have revolutionized the manufacturing and service sectors. What could they possibly do for information security management?

Because integrity is a central tenet of information security, we might, for instance, look to Six Sigma's goal of reducing errors to 1.4 (or less) per million operations. Given the sorry state of security in the average corporation, that is a noble but lofty goal indeed! Wouldn't it be fantastic if, say, we could cap security

Tip: If the scope of a change project changes, the projected costs *and* benefits need to be reassessed. Cutting the scope to cut costs is a common response when the budget is exceeded, but it also reduces the projected business benefits from the cancelled or modified functions to be delivered. Updating the projections is doubly important if the anticipated business benefits will be used as metrics once the change is implemented.

	Software Security Metric	PRAGMATIC Ratings (%)									
		Predictive	Relevant	Actionable	Genuine	Meaningful	Accurate	Timely	Independent	Cost	Score
12.1	Software security maturity	S M	90	95	70	80	90	85	90	90	86%
12.2	Percentage of controls tested realistically	M	92	95	90	65	95	60	75	55	60
12.3	Software quality assurance	M	83	85	91	73	90	68	70	80	20
12.4	Quality of system security revealed by testing	M	83	88	83	73	90	68	80	82	10
12.5	Extent to which information security is incorporated in software QA	M	85	80	67	62	70	50	35	35	50
12.6	Extent to which QA is incorporated in information security processes	M	75	70	66	61	80	50	35	36	50
12.7	Percentage of configuration items in line with service levels for performance and security	M O	60	75	65	62	40	70	35	80	20
12.8	Percentage of technical controls that fail safe	M	59	55	66	78	77	33	20	48	10
12.9	Number of deviations identified between configuration repository and actual asset configurations	M O	50	60	60	64	40	50	40	60	20

vulnerabilities in computer software to no more than 1.4 security-relevant design flaws or bugs per million lines of code? We may be well short of this today, but there is no obvious reason why Six Sigma concepts could not be applied consistently across the IT industry—and despite the vast ocean of mediocrity that surrounds us, we are convinced there is actually a viable commercial market for high-quality, secure software.

Another line of quality thinking is quality of security services (QoSS). While there have been some esoteric developments behind QoSS, it is not a mainstream practice for most organizations, and few information security managers would claim to be familiar or conversant with it. The underlying notion is that the quality or strength of security translates into cost and can be varied as is sufficient to conserve resources, meaning computational overhead and, of course, money.

While few would argue against improving the quality of just about anything of value, whether quality makes sense as a measure of security is uncertain. Certainly, the quality of performance of critical security procedures looks like a useful metric. It could be said that quality is closely related to compliance: a very high level of procedural compliance implies a high-quality process, albeit with the caveat that the procedure is not inherently flawed.

Truly achieving quality across the human, process, and technology dimensions is great, but in many cases, the *perception* of quality is even more important and may, in fact, be the better metric. From a customer perspective, purchasing a quality product from a quality organization is a satisfying experience, which is good for business. There are parallels with security in that the perception of strong security may deter casual attacks. However, regardless of perceptions, both security incidents and quality failures can destroy trust.

The IT systems and networks on which most business processes now depend are constantly being updated and modified, and hackers, fraudsters, and malware authors are forever finding new technical and procedural weaknesses to exploit. Technical vulnerability management, then, is typified by the hamster wheel of pain that is patching.

Example Security Metric 12.1

Software security maturity	P	R	A	G	M	A	T	I	C	Score
	90	95	70	80	90	85	90	85	90	86%

As usual, please look up the maturity scoring scale behind this example metric in Appendix H. Notice that in the summary table, we have classified the metric “S M,” meaning it probably has value for both strategic and management-level decision-making purposes, but perhaps not for lower-level operational decisions. We have classified all the example metrics by strategic/managerial/operational (SMO).

Tip: If you found yourself hunting for security metrics for senior management to support their strategic-level security planning, filtering out just the strategic metrics from the metrics catalog would make your job easier. As we said in Section 6.5, there are many different ways to classify metrics: SMO is simply the categorization we chose to illustrate the technique.

Example Security Metric 12.2

Percentage of controls tested realistically	P	R	A	G	M	A	T	I	C	Score
	92	95	90	65	95	60	75	55	60	76%

Testing security controls is important because they tend to regress or degrade naturally over time, while untested controls may not operate as expected and may not meet control objectives. We have rated this metric highly because it picks up on an issue we believe is far more widespread than it ought to be. The information security profession places a lot of emphasis on the specification, design/selection, and implementation of security controls addressing identified risks but pays scant attention to testing those same controls both prior to implementation and later when in operation, hence ensuring that an acceptable level of control is both achieved and maintained.

To be fair, though, the use of terms such as “realistically” could be the death knell for certain metrics in some organizations. You and I might understand perfectly well what we mean by realistic controls testing. We might feel it is obvious that we mean to discount trivial reviews and other nonscientific tests. However, an astute manager might take us to task for being so vague and, in so doing, may devalue or even discredit our metric.

Tip: As you get more and more serious about this, you will soon come to appreciate the sometimes subtle nuances of interpretation that can turn an otherwise beautifully elegant security metric on paper into a complete train wreck when presented to and discussed by management. Be careful about the language in which you express and explain your chosen metrics and, if they are not crystal clear, take the time to explain them to and discuss them with your audiences. By all means put formal descriptions of the metrics in an appendix to your security reports or on a Web page tucked away on information security management’s intranet security zone, and don’t be shy about referring to them if people start to query their true meaning. On the other hand, wouldn’t it be better to rephrase evidently obscure or confusing metrics such that they are, indeed, crystal clear?

Example Security Metric 12.3

Software quality assurance	P	R	A	G	M	A	T	I	C	Score
	83	85	91	73	90	68	70	80	20	73%

We've cheated a bit with this example. Software QA is an entire field of professional practice, far more than just a single metric. We've included it in this chapter for two good reasons: (1) QA is potentially a very powerful means of ensuring that developed software meets defined security objectives or requirements, and (2) it can generate a vast spectrum of fascinating metrics about the development process.

Key to making this metric work really well is to treat security as an aspect or feature of the software that is potentially every bit as important and valuable to the end user as other, more obvious, aspects, such as functionality, performance, utility, and aesthetics. In the same way that software architects and designers typically generate "use cases" describing how the software is anticipated to be used, security architects and designers can generate "misuse cases" describing how the software is anticipated to be attacked, compromised, or otherwise misused (McGraw 2006).

{Metric 12.3} measures software QA as a whole, not specifically the information security elements, on the assumption that a sound approach to QA is a solid basis for necessary information security activities. To turn that on its head, imagine trying to develop secure software using a process that completely lacks the QA mentality: it would be a sheer nightmare.

Example Security Metric 12.4

Quality of system security revealed by testing	P	R	A	G	M	A	T	I	C	Score
	83	88	83	73	90	68	80	82	10	73%

Don't be misled by the word "quality" in this example: {metric 12.4} concerns system security *testing*, which is a form of quality control (QC), not the QA we have just been discussing. In a manufacturing context, QC involves testing products for defects as they approach the end of the production line. As such, QC is rather inefficient and expensive compared to QA's build-quality-in approach because products at that late stage of production have gained almost all their value. If they cannot be reworked to fix the identified defects, the only sensible option is to discard them.

On the other hand, in the absence of QA, QC is probably better than releasing defective products!

The metric implies that system security is in some way measured by the testing process. The raw data for this metric might arise from, for instance, security bug, defect, or vulnerability reports generated by security tests performed either as part of regular unit, system, integration, and production acceptance testing or, of course, discrete security/penetration tests. The number of security issues would be a rather crude metric, but it is not hard to envisage more sophisticated and useful versions, perhaps analyzing the

Tip: This metric could easily end up being a highly sophisticated and complex set of measures, for instance, combining capability maturity model approaches with defect/root cause analysis, surveying project managers regarding their interactions with information security, and a whole bunch more. Luckily, it is feasible to start small with relatively simplistic, even subjective measures and let this metric evolve naturally under its own steam in line with evolving security practices on the software development projects being measured.

issues by their severity (which is really another way of saying risk) and nature (e.g., do they chiefly affect confidentiality, integrity, or availability?). Going the other way, the ultimate security test metric is the final pass/fail!

Example Security Metric 12.5

Extent to which information security is incorporated in software quality assurance	P	R	A	G	M	A	T	I	C	Score
	85	80	67	62	70	50	35	35	50	59%

We have already mentioned that information security is highly relevant to, and should be considered throughout, the systems development lifecycle from feasibility right through to system retirement/replacement. {Metric 12.6} aims to determine how closely information security is integrated into and supports the software lifecycle through QA activities. Is security merely an afterthought in the process, or are security activities performed routinely in much the same rigorous and comprehensive manner as, say, functional requirements analysis, development, and testing?

Example Security Metric 12.6

Extent to which quality assurance is incorporated in information security processes	P	R	A	G	M	A	T	I	C	Score
	75	70	66	61	80	50	35	36	50	58%

Ignore the confusingly similar wording to the preceding example for a moment: this is a totally separate metric. The premise for this metric is that QA is applicable to information security processes. The quality of information security products, such as security risk assessments, architectures, and designs, significantly influences the security achieved by the corresponding information systems and business processes. Quality concepts, such as fitness for purpose, right first time, and customer driven, apply to security activities and processes in much the same way as they do to goods and services in general.

Tip: In reality, it is generally a bad idea to report two or more distinct metrics that have such similar names. A confused audience is a distracted audience no longer focused on the meaning of the measures being reported or presented. Either rephrase one or both of the metrics or (with care) use nicknames that emphasize the differences.

Again, we are reluctant to describe the example metric in detail because it can grow to be highly sophisticated. Many QA activities directly involve or facilitate the generation of metrics, not least because measurement information is intended to be used to influence or control the processes concerned.

Example Security Metric 12.7

Percentage of configuration items in line with service levels for performance and security	P	R	A	G	M	A	T	I	C	Score
	60	75	65	62	40	70	35	80	20	56%

ISACA suggests a version of this metric presumably on the basis that failure to comply with security-related configuration requirements increases risk. We scored the metric low for **Meaning** because, as originally specified by ISACA, it reflects only the number of discrepant items, taking no account of their *severity*. In different situations, there may be loads of trivial issues or a few very significant ones: taken in isolation, ISACA's metric would be distinctly misleading, failing to indicate the rather substantial differences between these circumstances. It is not too hard to construct a more useful metric that would take account of both the number and the severity of the issues found, but doing so requires some subjective interpretation by the person doing the assessment, and the additional complexity would, of course, increase the **Cost** of the metric.

Example Security Metric 12.8

Percentage of technical controls that fail safe	P	R	A	G	M	A	T	I	C	Score
	59	55	66	78	77	33	20	48	10	50%

In conceptual terms, fail-safe is an application of contingency planning. Controls performing vital security functions can be designed and implemented in such a manner that if, for some reason, they fail in service, they leave whatever is being controlled in a controlled, secure, or locked-down state. It doesn't particularly matter *why* they failed.

Truck and train air brakes are the classic example of fail-safe engineering: air pressure is used to *release* rather than *apply* the brakes against spring pressure. If the

compressed air system springs a leak, the compressor fails, or a pneumatic brake pipe bursts, the brakes are applied automatically. Conversely, if air pressure was required to *apply* the brakes, air system failure for whatever reason would leave the vehicle without brakes.

In the technical security sphere, an equivalent might be a firewall that is configured to block all traffic by default. Only if it periodically receives instructions to pass a certain type of traffic will it open up the corresponding flow. If those instructions fail to arrive for some reason, it pinches off the flow and raises the alarm.

The example metric tells us what proportion of our technical security controls are designed and configured to be fail-safe. It is very unlikely that we would want *all* our technical controls to be fail-safe, but it is a fair bet that certain key controls should be fail-safe. Measuring and reporting the metric is one way to ensure this happens.

Example Security Metric 12.9

Number of deviations identified between configuration repository and actual asset configurations	P	R	A	G	M	A	T	I	C	Score
	50	60	60	64	40	50	40	60	20	49%

This is another ISACA-inspired metric. Both the number *and* the magnitude of deviations are indicative of risk levels, but as stated, the metric only takes account of their number.

7.10 Incident Management Example Metrics

Managing information security incidents competently can make the difference between the organization occasionally experiencing some noteworthy events as opposed to suffering a succession of avoidable incidents, serious compromises, or even a complete disaster.

There are options and potential issues at every stage of the incident management process:

- Preparing for incidents involves getting employees ready to identify and report incidents, a consistent and widely known reporting mechanism, and having resolving agencies ready to respond efficiently—and, of course, preventing incidents is usually preferable to suffering from and dealing with them!
- Reporting is vital because, otherwise, there is nothing to trigger the response.
- Incident response is an example of contingency management in action because the precise responses needed are contingent (depend) upon the nature of the incidents that unfold: being prepared for anything is easier said than done, however!

	<i>Incident Management Metric</i>	<i>Strategic, Managerial or Operational</i>	PRAGMATIC Ratings (%)						<i>Score</i>			
			<i>Predictive</i>	<i>Actionable</i>	<i>Genuine</i>	<i>Meaningful</i>	<i>Accurate</i>	<i>Timely</i>	<i>Independent</i>	<i>Cost</i>		
13.1	Information security incident management maturity	S M	90	95	70	80	90	85	90	86%		
13.2	Time taken to remediate security incidents	M	82	69	85	76	80	75	65	70	74%	
13.3	Time lag between incident and detection	M O	80	70	72	30	75	50	50	65	62%	
13.4	Percentage of incidents for which root causes have been diagnosed and addressed	M	85	85	67	40	77	40	48	40	55%	
13.5	Cumulative costs of information security incidents to date	S M	76	85	0	30	95	30	33	40	55	49%
13.6	Number of information security events and incidents, major and minor	S M O	70	60	0	50	72	35	35	70	50	49%
13.7	Number of information security incidents that could have been prevented, mitigated, or avoided	M	50	75	0	15	85	5	16	9	42	33%
13.8	Nonfinancial impacts of incidents	S M	60	65	0	20	60	6	30	20	17	31%

- Some incidents require the careful collection and analysis of forensic evidence following regimented, painstaking procedures, but that can slow down the examination and resolution, so there are often key management decisions to be made as part of the process, for example, do we keep the system offline while the incident is forensically examined or just clean it up and return it to service? This conundrum illustrates the inherent conflict between problem management that seeks to determine root causes and incident management that is generally tasked with speedy restoration of services and processes. It is prudent for the incident manager to ascertain management's perspective on issues of this nature in advance of—rather than in the thick of—a major incident, ideally developing flexible policies and procedures to codify management's intent and hopefully save time and grief on that fateful day.
- Resolving incidents is still not the end of the process: the best organizations systematically learn and improve as a result of incidents they have suffered and, for that matter, near misses and information security incidents experienced by third parties.

A generic security incident management process diagram is given in Figure 7.2.



Figure 7.2 Security incident management process.

Tip: Remember these are just example metrics to illustrate the PRAGMATIC scoring method. The scores reflect *our* understanding and *our* interpretation of the value of the example metrics in *our* hypothetical context. We are quietly confident that most other information security professionals will come up with broadly similar scores and rankings by following the method, and we invite you to prove us wrong. Go ahead, make our day. Seriously, we'd like to know if the method is broken. If you can help us fix it too, we'd be delighted!

The example metrics in this section are based on the kinds of things that we have seen being measured in relation to incident management practices.

Example Security Metric 13.1

Information security incident management maturity	P	R	A	G	M	A	T	I	C	Score
	90	95	70	80	90	85	90	85	90	86%

You know the drill—see Appendix H.

Clearly having created, used, and developed them, we like our maturity scales, but maybe, just maybe, we have been a teensy weensy bit biased in our PRAGMATIC scoring of the maturity metrics. They all score quite well in our opinion, but you may beg to differ. *Please* don't take our word for it. If they score badly for you in your context, they probably won't work well in practice.

Example Security Metric 13.2

Time taken to remediate security incidents	P	R	A	G	M	A	T	I	C	Score
	82	69	85	76	80	75	65	75	60	74%

Remediation time appears to be a simple yet effective measure of the organization's incident response capability. Remediation, in this context, means the point at which an information security incident—or, more precisely, an incident, event, or adverse situation having a substantial information security element or cause—is considered resolved. This is generally indicated by the original tickets being closed on the incident management/tracking system and may not extend as far as the post-event investigation and learning activities, important though they undoubtedly are: the reason is that they are far less time-critical in most cases.

Example Security Metric 13.3

Time lag between incident and detection	P	R	A	G	M	A	T	I	C	Score
	80	70	72	30	75	50	50	65	65	62%

Lag times are not always clear cut, but good forensics can increase precision. The frequency with which this metric is analyzed and reported creates a lag between the measured activities and the information reaching management, in much the same way as there is a lag between incidents occurring and their being detected. It also affects the quality of the information (moving averages are more representative over a longer period, smoothing out short-term variances) and the costs associated with the metric. This issue is, of course, common to other periodic metrics and clearly needs to be taken into account in the metric design and implementation process. Furthermore, it is sensible to revisit this issue from time to time because, as the organization's approach to information security management matures, more frequent/granular metrics may be of greater utility.

A possible variant of this metric involves measuring the time lag between incident detection and resolution. This would seem to encompass the remaining core parts of incident management, but there's a nasty problem: many incidents are never actually resolved. Some never get investigated for a variety of reasons. Some are found to have arisen from so-called one-off or hundred-year risks that are thought to be extremely unlikely ever to recur. Some are impracticable or too costly to address, meaning management is prepared to accept the risk.

A further nuance of this metric is that some incidents are never detected. Many minor and a few more major frauds no doubt fall into this category. The same is true with accidents, such as typos. Focusing all the organization's energies on speeding up the detection of security incidents may prove counterproductive if it raises the detection floor, so even more incidents pass unnoticed.

Example Security Metric 13.4

Percentage of incidents for which root causes have been diagnosed and addressed	P	R	A	G	M	A	T	I	C	Score
	85	85	67	40	77	40	48	16	40	55%

It is patently obvious that failure to determine the true causes of security incidents and, hence, failure to address those causes in a systematic manner practically invites them to recur. On the other hand, deep analysis of almost any incident almost invariably reveals a plethora of causative or contributory factors aside from the more obvious but superficial things that anyone can see. A powerful technique often used in quality circles is to keep on asking "Why?" and probing still further as each cause is uncovered, exploring deficiencies further and further back through the layers behind the process until that line of inquiry, along with the investigatory team, is completely exhausted. Again, this metric is likely to evolve along with the organization's security maturity. In the early stages, even those superficial findings from initial inquiries may be of interest and concern to a management that is broadly oblivious to the organization's security failings.

Once it starts addressing and trying to resolve the issues, its information needs will change.

Example Security Metric 13.5

Cumulative costs of information security incidents to date	P	R	A	G	M	A	T	I	C	Score
	76	85	0	30	95	30	33	40	55	49%

Although the business costs of incidents are extremely useful for anyone developing business cases or budgets for information security activities, these are extremely hard (read: expensive) to ascertain in practice. The direct costs of incidents (e.g., incident investigation and legal costs) are normally recorded in some form by those involved and, hence, are relatively straightforward to determine, but the indirect costs (e.g., customer defections, brand devaluation, lost business opportunities) are far more cryptic, basically coming down to highly subjective interpretations and projections from limited available information. The problem is that indirect costs *may* be substantive following serious incidents (perhaps substantial enough to warrant formal reporting to stakeholders), but in truth, nobody knows for certain.

While it is unrealistic for anyone to expect that incident management will completely eliminate all the costs arising from information security incidents, it is reasonable for management to anticipate a reduction in incident-related costs compared to not having an incident management process: the thorny problem, of course, is how to determine what would have happened if there was no such process. There are two cost elements to consider:

1. The impacts caused by the incidents being managed: identifying, responding to, and resolving incidents as soon and as effectively as possible should, of course, minimize these costs. Aside from its use to evaluate the process, reliable information about the actual costs of incidents is valuable for many purposes, for instance, to make future risk assessments more accurate and perhaps to target improvements in specific information security controls mitigating the costliest incidents. We recommend tracking and reporting incident-related costs as a key metric. Examples include man-days spent on each incident by the incident management team and support crew; costs incurred in replacing hardware, reloading software, regenerating lost data, etc.; and business costs incurred by loss of IT services while incidents are resolved.
2. The costs of building and maintaining the incident management function and operating it during actual incidents: Optimizing the incident management processes while actively tracking and managing the associated costs should help keep them under control. The initial setup costs could be treated as a typical capital investment with a projected return: A well-written business case or investment proposal is an ideal source of metrics to track. The costs of running the process can be tracked using conventional budgeting and time recording processes.

Tip: Start collecting data on incident costs and impacts as soon as possible, even if it's done somewhat informally and haphazardly at first. Trust us: as you start to accumulate dollar figures based on the real-world costs of security failures, you will soon find opportunities to use your data to help justify security measures. Before long, a positive feedback loop will kick in and your data collection and analysis will mysteriously improve: at much the same time, your cumulative cost curve should see a gradual reduction in the rate of increase.

Historical measurements of incident costs prior to establishing the process (if you are fortunate enough to have them) may give a baseline for comparison once it is up and running, but this approach is tricky because of the variability of information security incidents. Furthermore, the very presence of an incident management process typically means more incidents end up being proactively managed, while the associated incident and management costs are more likely to be accounted for.

Example Security Metric 13.6

Number of information security events and incidents, major and minor	P	R	A	G	M	A	T	I	C	Score
	70	60	0	50	72	35	35	70	50	49%

The concept lurking behind this relatively simple metric is that someone who is prepared to steal a dime may steal a dollar; in other words, even minor incidents should be of concern to management as they may be indicators or precursors to something more serious. Few network hacks come totally out of the blue, for example: most involve enumeration activities in which target networks and systems are quietly probed for characteristics and vulnerabilities that will be exploited in due course. Being alert for such early-warning activities, even though they seem trivial in isolation, may give you just the edge you need to stave off an impending attack. A metric that counts them is one way to remind everyone that they are not *all* merely background noise, although, admittedly, we are still left with the problem of sifting the wheat from the chaff.

Example Security Metric 13.7

Number of information security incidents that could have been prevented, mitigated, or avoided	P	R	A	G	M	A	T	I	C	Score
	50	75	0	15	85	5	16	9	42	33%

Tip: Open, honest, forward-looking post-incident reports are generally more productive than this rather crude numeric example metric, assuming, of course, that post-incident reports are actually compiled and circulated (which, unfortunately, is by no means a universal security practice).

As stated, {metric 13.7} is a poor example. Although one might argue the metric stimulates people to evaluate incidents, it is rather subjective and ill-defined. With hindsight, virtually every incident could have been prevented, mitigated, or avoided because the necessary actions or controls tend to be obvious after the fact. Consequently, the evaluation may be superficial, being curtailed as soon as it is established that, indeed, *something could have been done to stop it*.

The metric itself is not very informative. What does the number actually tell us? What is the ideal number, and what should be done if the number gets too high?

Worse still, the metric may encourage a blame culture if it leads managers to argue over who *should* have prevented, mitigated, or avoided incidents. There be dragons.

Example Security Metric 13.8

Nonfinancial impacts of incidents	P	R	A	G	M	A	T	I	C	Score
	60	65	0	20	60	6	30	20	17	31%

We have already noted that the indirect costs of incidents are very difficult to quantify in a rational, defensible manner. It would be even more of a problem to try to measure the nonfinancial impacts—and it could be argued that, in any case, they are irrelevant to a classical commercial organization whose *raison d'être* is to turn a profit. Even defining what is meant by nonfinancial impacts is tricky. In short, this is a classic example of a metric that creates more issues than it resolves. It may conceivably have some security awareness value in stimulating the inevitable ensuing discussion, but there are much better ways of doing that than presenting such vague and easily dismissed metrics.

Cumulative cost and impact metrics score surprisingly poorly on the PRAGMATIC scale for a number of reasons relating to the time and effort needed to gather the data. The direct costs of an incident—things such as the book value of information assets lost or damaged and the costs involved in managing, investigating, and resolving the incidents—are relatively simple to collate (although few organizations even bother to do that!), but the consequential business costs that are usually more significant—things such as damage to reputations and brands—are much harder to determine with any accuracy. However, these metrics score very highly in terms of meaning to management: knowing the organization lost \$X million last year through information security incidents could be exactly the ticket for the information security manager to be allocated the resources needed to bring the losses down.

Tip: Consider the impact on share value, taking into account variations in overall market value before and after a significant incident, perhaps relative to a close competitor. For example, if your organization had a market value twice that of a close competitor before a major incident but was reduced to the same market valuation and all other factors were the same, you have a strong argument as to the value of the reputational damage.

7.11 Business Continuity Management Examples

We'd like to point out up front that our interpretation of business continuity management goes well beyond DR planning, taking in aspects such as resilience, business resumption, and true contingency planning. This may come as something of a shock to anyone who considers ISO/IEC 27002 a best practice standard! DR planning is an important part of the mix, to be sure, but other aspects are equally, if not more, important and, in our experience, much neglected outside of organizations that have developed a mature, comprehensive, and professional approach to business continuity management.

We define business continuity as an approach to ensuring operational activities that are considered essential to the business either *continue to operate* despite incidents or else are *recovered* before the impacts of unplanned outages become excessive. The definition implies that we know which business activities are, in fact, *essential* (because the costs of maintaining or recovering *all* activities could be prohibitive), and we understand at what point impacts would become *excessive*. Both aspects are addressed through assessing business continuity risks, the process commonly known as *business impact analysis*.

Making the organization highly *resilient* is arguably the *ideal* way of ensuring business continuity. Resilience lets us shrug off incidents that might otherwise interfere with or stop vital business activities, keeping operations running without a noticeable break in service.

Following crisis management activities that we hope bring order to the chaos in the immediate aftermath, *disaster management* involves someone suitable taking charge of the activities that will follow a serious incident or disaster. In such a situation, capable managers are anticipated to take stock of what has happened, marshal their resources, then initiate and lead/direct the activities needed to recover or resume business operations. Needless to say, it is an extremely stressful job.

DR and business resumption planning start with the assumption that, despite our best endeavors, business processes may be disrupted. It could be that we were not sufficiently robust to withstand the event or sufficiently resilient to bend and not break (e.g., a supply chain failure that was totally out of our control and for which

			PRAGMATIC Ratings (%)							
			Actionable	Genuine	Meaningful	Accurate	Timely	Independent	Cost	Score
		<i>Business Continuity Metric</i>								
14.1	Coverage of business impact analyses	S M	95	90	99	90	95	80	86	88
14.2	Business continuity management maturity	S M	90	95	70	80	90	85	90	89%
14.3	Percentage of critical business processes having adequate business continuity arrangements	M	85	97	93	84	89	75	85	75
14.4	Percentage of business processes having defined RTOs and RPOs	M	88	99	90	68	93	68	92	84%
14.5	Business continuity plan maintenance status	M O	75	75	90	73	84	76	80	77
14.6	Disaster recovery test results	S M O	83	80	85	91	92	75	75	81
14.7	Uptime	M O	84	97	66	78	94	61	79	47
14.8	IT capacity and performance	S M O	92	92	82	77	96	62	84	64
14.9	Mapping critical business processes to disaster recovery and business continuity plans	S M	85	92	79	81	90	70	75	40
14.10	Business continuity expenditure	S M	75	92	20	82	95	70	70	70
14.11	Proportion of critical systems reviewed for compliance with critical control requirements	O	62	53	68	36	5	69	34	33

there were no viable alternative sources of supply), or maybe the resilience measures turned out to be inadequate in practice (perhaps it was a more serious incident than we were prepared for). It could also be that the incident was totally unanticipated and caught us on the blindside.

Well-managed organizations are capable of reacting efficiently and effectively to more or less any situation that occurs. The capability, willingness, flexibility, and resourcefulness to cope positively with whatever takes place could itself give a competitive advantage—and not only under disaster conditions. It might even be considered a strategic goal. True *contingency planning* assumes that unusual and often rather extreme incidents will still occasionally occur despite all the avoidance, preventive, resilience, and recovery measures employed. Perhaps the specific circumstances that transpire will be totally novel, or the controls will fail or be overwhelmed by a coincidence of events. Contingency planning sets about establishing the capability to identify, react, and respond effectively under all foreseeable circumstances. The most important element is the people—for example, encouraging them to be able to think for themselves, to collaborate in ad hoc teams when the situation demands, and to know when it is appropriate to bend or break the rules. It also involves storing away supplies, tools, information, and other resources that are likely to prove useful in a contingency situation—things such as duct tape and superglue, tools such as adjustable wrenches, food and water, spare parts, and contact details for people and organizations that might be able to help (e.g., specialist companies that can restore equipment damaged by fire or flood).

Example Security Metric 14.1

Coverage of business impact analyses	P	R	A	G	M	A	T	I	C	Score
	95	90	99	90	95	80	86	80	88	89%

Assuming the organization has a reasonably comprehensive inventory or map of its business process landscape, it would be interesting to report how much of that landscape has been analyzed for the potential business impacts of foreseeable information security incidents. While it would be simpler to report the number or proportion of systems and processes that have been impact-assessed, introducing assurance would subtly alter this metric by emphasizing management's confidence in the assessment results. There may be some value in comparing the information security manager or business continuity manager's personal assessment with those of the relevant information asset owners, identifying situations perhaps where there are lingering doubts about the quality or coverage of the impact assessments.

Example Security Metric 14.2

Business continuity management maturity	P	R	A	G	M	A	T	I	C	Score
	90	95	70	80	90	85	90	87	90	86%

See Appendix H for a maturity matrix to score the organization's business continuity management practices.

Example Security Metric 14.3

Percentage of critical business processes having adequate business continuity arrangements	P	R	A	G	M	A	T	I	C	Score
	85	97	93	84	89	75	85	85	75	85%

This is yet another example metric that uses a potentially ambiguous term, "adequate." It could have read "suitable" or "authorized" or something, but the specific term is not really the issue here—it's a matter of determining whether or not enough has been done to prepare for disaster, which is surely subjective, up until the point a disaster actually occurs anyway and we get to find out for sure.

There is an implicit risk with examples such as {metric 14.3} that politically astute managers may play games with it, especially if the metric is used rather aggressively by management to get things going and push things forward. Let's imagine the sales department has been a bit tardy in first specifying their business continuity requirements and then remiss in funding the work necessary to achieve the stated aims. Along comes the security guys with a metric pointing out that sales is way behind the curve on business continuity, and the C-suite starts clamoring for action or baying for blood. The head of sales has a choice: either divert resources from sales (which, naturally enough, occupies most of his or her working hours and almost completely fills his or her field of view) to business continuity (which, from his or her perspective, is all about remote "what if" scenarios and ridiculous scare stories originated by the paranoid freaks in the risk department!) or cut back on the business continuity requirements by pretending that various activities are not truly critical and can happily be put on hold for days or weeks. Artificially downgrading the specification of adequate business continuity arrangements is one way to improve the metric without actually improving security.

Tip: Read *You Are What You Measure* (Hauser and Katz 1998) or even *The Prince* (Machiavelli) if this scenario seems a bit far-fetched to you, you being a highly ethical information security professional who always plays by the rules.

Example Security Metric 14.4

Percentage of business processes having defined RTOs and RPOs	P	R	A	G	M	A	T	I	C	Score
	88	99	90	68	93	68	92	68	90	84%

Recovery time objectives (RTOs) and recovery point objectives (RPOs) are commonly used business continuity parameters, defining the key business requirements for recovering failed business processes and thus the supporting services, networks, systems, supplies, people, etc. Your organization may use different acronyms or different parameters, but that's a minor issue: the metric concerns what proportion of business processes have documented business continuity requirements, howsoever defined.

This metric works well as a means of bootstrapping the business continuity management processes. It is **Meaningful**, **Actionable**, highly **Relevant**, and **Timely** in that once key business continuity parameters have been determined, defining the business requirements, a load of activities can proceed at full steam. If instead the parameters are missing in action, most of the downstream activities are stuck in limbo.

Example Security Metric 14.5

Business continuity plan maintenance status	P	R	A	G	M	A	T	I	C	Score
	75	75	90	73	84	76	80	77	93	80%

This metric could be a simple count of the number of plans that have not been reviewed/tested when those reviews or tests should have taken place or the total number of days they are overdue. Crudely ranking all available BC plans according to the time since they were last reviewed/updated will identify any that have never been reviewed/updated (excluding new ones) and any that have not been reviewed/updated in ages, indicating that they are not being actively maintained and are probably out of date and possibly no longer satisfactory. Better yet, if review/update periods are routinely defined for BC plans, it is possible to identify and report BC plans whose review/update is due or overdue, creating a richer and more useful management metric. An important consideration is that the main cause of BCP/DRP failure is the result of failing to keep plans current.

Tip: Try to find a way to report BC plans that have not yet been created or have mysteriously gone missing in action; otherwise, the tendency is to avoid being chased for plan updates by claiming the plans are no longer required and have been retired. And yes, people really do play these crazy games!

Example Security Metric 14.6

Disaster recovery test results	P	R	A	G	M	A	T	I	C	Score
	83	80	85	91	92	75	75	81	60	80%

Organizations vary widely in the type of DR reporting they use but, generally speaking, senior management value simple, high-level, pass/fail reporting while more detail is needed for lower levels, right down to the specific technical and procedural information required by operational people to update DR arrangements. Organizations that routinely specify parameters, such as RTO, RPO, service delivery objective (SDO), maximum tolerable outage (MTO), and allowable interruption window (AIW) have obvious benchmarks against which the DR arrangements should be validated and reported. Aside from merely creating and maintaining DR plans, they need to be tested and exercised for assurance and awareness purposes, respectively. Tabletop run-throughs have their place, but the highest levels of assurance in the organization's DR arrangements can only be achieved either by testing them thoroughly in shockingly realistic scenarios or by actually using them for real (which is definitely not an option we'd recommend!). The metric should preferably reflect both DR and assurance requirements, for instance, providing a color-coded heat map using green for requirements fully satisfied, yellow for requirements partially satisfied, and red for requirements unsatisfied, and using white for requirements unspecified—or abject surrender to the forces of evil.

Example Security Metric 14.7

Uptime	P	R	A	G	M	A	T	I	C	Score
	84	97	66	78	94	61	79	47	89	77%

Tip: Uptime is a fascinating metric for IT services delivered from the cloud. The business IT user doesn't particularly care whether an IT service failure was caused by the IT department, the network providers, or by one or more cloud-service providers. All that matters is that it is fixed up quickly so the business process can resume, and ideally it is fixed properly such that it won't fail again. As with the just-in-time production lines in a modern factory, the whole process can become fragile as a result of the possibility of failures in any part, including those that occur outside the organization's boundary fence. Measuring the whole thing promotes a customer focus and encourages more cooperation between the various parties involved to achieve service levels that business users need (or rather, whatever they are willing to pay for!).

“Uptime” is the classic availability and service measure for the IT department, alongside variants and derivative measures, such as total or unplanned downtime and number and severity of outages. Most IT departments and ICT service providers track and report it in some fashion. Most also interpret uptime as liberally as they conceivably can, for instance, excluding planned outages (typically including backups, patches, and changes) as if they somehow don’t interrupt IT services, which, of course, they do. From a strict information security perspective, the liberal service provider version of uptime may not be entirely appropriate.

Example Security Metric 14.8

IT capacity and performance	P	R	A	G	M	A	T	I	C	Score
	92	92	82	77	96	62	84	64	29	75%

Although presented as a single example metric, capacity and performance within IT are actually measured by a whole family of metrics in practice. They qualify as an information security metric because capacity and performance are closely related to uptime and, hence, availability.

We marked this metric down on Accuracy because it is often a hot potato in any IT department that is ruled by its service-level agreements or contracts, meaning the data are manipulated for political reasons.

Example Security Metric 14.9

Mapping critical business processes to disaster recovery and business continuity plans	P	R	A	G	M	A	T	I	C	Score
	85	92	79	81	90	70	75	40	40	72%

Here, we envisage some sort of physical overlay on the business process landscape/map noted earlier, showing both the extent to which DR and BC arrangements cover the landscape and the status of those arrangements, particularly in relation to the most critical business processes. A heat map might, for instance, indicate areas that have achieved a complete pass (green); a partial fail (yellow); or a severe fail, untested or unspecified (red), in each case, comparing the resilience and recovery test results achieved against the corresponding business continuity requirements as specified by the information asset owners. Further details could be provided to substantiate the reported values, for example, business continuity sign-offs from the information asset owners for the greens, allocated action plans for the yellows, and, for the reds, either proposals to address them or at least statements identifying the people responsible for developing the proposals. Provided it is carefully defined and applied, reporting on DR/BC arrangements that are suitable would give senior management a more strategic overview of the organization’s BC

232 ■ PRAGMATIC Security Metrics

status. With a bit more sophistication, this metric could be turned into a process maturity metric, distinguishing systems/processes where the business continuity requirements are merely defined from those which are defined and in place and, ultimately, from those which are defined, in place, and proven. A single “percentage covered” number would be simpler to report but would have much less impact and value to the recipients because it would lack those vital details about which processes or areas remain exposed.

Example Security Metric 14.10

Business continuity expenditure	P	R	A	G	M	A	T	I	C	Score
	75	92	20	82	95	70	70	70	70	72%

You might think this would qualify as a must-have security metric because the total expenditure on business continuity is likely to be of great concern to management. Unfortunately, however, it has a number of drawbacks that rather take the gloss off it, most notably the fact that it ignores the substantial business benefits of business continuity.

Example Security Metric 14.11

Proportion of critical systems reviewed for compliance with critical control requirements	P	R	A	G	M	A	T	I	C	Score
	62	53	68	36	5	69	34	43	33	45%

Aside from the rather vague wording of this example metric, which drastically affects the **Meaningful** score, it doesn’t score particularly well in the other PRAGMATIC criteria either with the net result that it achieves a mediocre overall score.

We could just leave it at that and, in effect, abandon this metric because there are so many higher-scoring metrics to consider. On the other hand, we could dig a bit deeper into the reasons why it scores so badly, perhaps developing and scoring some variant or derivative metrics along the same lines to see if we can find something better.

7.12 Compliance and Assurance Metrics Examples

Before we proceed to evaluate possible security compliance and assurance metrics, here are a few factors to consider:

- Is compliance truly a binary issue (one is either compliant or noncompliant), or is it analogue (one may be largely compliant or barely compliant; one may be more or less compliant than another)?
- How much compliance is really needed and appropriate? Is it reasonable to demand full compliance under all circumstances? Is it even feasible to expect this?

(Continued)

	<i>Security Compliance and Assurance Metric</i>	PRAGMATIC Ratings (%)										
		Score			Cost	Independent	Timely	Accurate				
		Genuine										
		Meaningful										
		Actionable										
		Relevant										
		Predictive										
15.8	Number of unapproved/unlicensed software installations identified on corporate IT equipment	M	58	55	82	73	86	47	64	66	17	61%
15.9	Percentage of security policies supported by adequate compliance activities	M	96	92	78	40	75	33	60	34	30	60%
15.10	Compliance benchmark against peers	S M	80	65	62	61	90	60	22	65	10	57%
15.11	Number or rate of security policy noncompliance infractions detected	O	55	64	75	50	68	34	59	76	33	57%
15.12	Embarrassment factor	S M	26	38	20	50	63	72	40	87	87	54%
15.13	Percentage of purchased software that is unauthorized	M	71	51	90	75	82	35	13	20	6	49%
15.14	Proportionality of expenditure on assurance versus potential impact × likelihood	M	65	40	85	40	3	20	46	76	35	46%
15.15	Proportion of software licenses purchased but not accounted for in repository	M O	1	1	90	84	1	70	50	81	30	45%
15.16	Percentage of critical information assets residing on fully compliant systems	M	48	26	36	41	56	13	19	46	12	33%

- Likewise with assurance: how important is it to be certain that management knows the truth about and understands information security?
- Are the predicted consequences of perhaps being caught and sanctioned at some future point for noncompliance (taking into account direct and indirect/consequential costs and the likelihood that we may be forced into making changes to achieve compliance under pressure rather than as we choose) less than the costs of achieving compliance today?
- Is compliance primarily a business, risk management, ethics, or some other kind of issue? Why should we be concerned at the extent of compliance? Does it really matter if we are not fully compliant?
- Does enforcement always help? Or is there an optimal level of enforcement beyond which there are diminishing returns, not to mention general aggravation and resentment from employees who feel they are being pushed too hard?*

Those questions exemplify the kinds of thought processes you should follow to clarify the organization's business objectives for and interest in the information security controls in each area because the objectives will drive the selection of appropriate metrics and the rejection of inappropriate or unhelpful metrics. In other words, there is no point measuring factors that are of no concern to anyone.

Now, let's move on to evaluate some example security compliance and assurance metrics.

Example Security Metric 15.1

Information security compliance management maturity	P	R	A	G	M	A	T	I	C	Score
	90	95	70	80	90	85	90	85	90	86%

As usual, we envisage using a maturity scoring scale vaguely similar to that suggested in Appendix H.

Example Security Metric 15.2

Breakdown of exceptions and exemptions	P	R	A	G	M	A	T	I	C	Score
	87	83	84	94	81	83	84	87	88	86%

Situations, processes, activities, and systems that do not comply with applicable information security policies, procedures, standards, laws, regulations, etc., fall into one of two camps: either the noncompliance has been officially sanctioned

* People generally behave better when they think it is to their benefit, especially if they believe they are being watched and know noncompliance will lead to adverse personal consequences. Comparing compliance metrics before and after a slew of enforcement actions provides the guidance for management to optimize the compliance and enforcement mix.

236 ■ PRAGMATIC Security Metrics

by management (which we call *exemptions*, meaning they have been explicitly exempted from the requirements), or not (meaning *exceptions*).*

Example Security Metric 15.3

Number and severity of findings in audit reports, reviews, assessments, etc.	P	R	A	G	M	A	T	I	C	Score
	79	89	87	96	92	84	30	96	36	77%

The number and severity, gravity, or nature of audit findings pertaining to information is an indication of the (a) maturity of the organization, (b) maturity, coverage, and quality of security controls, and (c) depth of audit. If this metric shows an improvement in successive measures, things are clearly getting better—and vice versa. Therefore, it can be a useful high-level or strategic metric, particularly as it is highly independent and, hence, a genuine measure, unlikely to be substantially manipulated by someone gaming the system.

You may think it is better to distinguish those audit findings that specifically relate to information security, but that potentially opens a can of worms concerning how the findings are categorized and introduces more subjectivity. It could be argued that practically everything auditors report does relate to information security in some fashion, and at the end of the day, management is not solely concerned with information security, so does it really matter anyway?

Example Security Metric 15.4

Status of compliance with externally imposed information security obligations	P	R	A	G	M	A	T	I	C	Score
	77	85	85	70	98	68	35	89	60	74%

Third parties impose a variety of information security requirements or obligations on the organization through legal, regulatory, contractual, or ethical means. Managers, especially senior managers or officers, have a particular interest in ensuring the organization should avoid being caught in noncompliance with certain obligations because they may be held personally accountable by the authorities, on top of being held to account by senior management for the organization's liabilities. It is rather naïve to assume that full compliance is essential in every case. Compliance with externally imposed obligations is, in a sense, a risk-management activity. Management can weigh the possibilities and likely costs of being caught and sanctioned for noncompliance, offsetting those against the likely costs of

* Potentially, there could be situations in which an exemption has been approved but is not properly applied in accordance with the authorization or other security requirements. We would class that as an exception.

Tip: Compliance with externally imposed information security obligations usually involves some form of audit or assessment, meaning information (not necessarily numeric metrics) should be readily available for areas that have been compliance-assessed. The review and reporting costs are likely to be substantial, but they are generally required for business reasons aside from just gathering information security metrics; information security management gets a free ride with these metrics.

achieving full compliance. In a similar fashion, the cost of measuring and reporting this metric is offset by the value of management discovering the organization's compliance status internally rather than through a report from an auditor, regulator, or judge (no surprises!).

Organizations are not normally *obliged* to comply with them,* but if management understands and sees value in good practice information security models, frameworks, and standards, such as BMIS (see Appendix B), Zachmann, TOGAF, SABSA, ISO27k, ITIL/ISO 20000, COBIT, and PCI-DSS, it may be worth comparing the organization's security practices and controls systematically against them, either in whole or in part (e.g., measuring and working on successive sections of COBIT in successive quarters).

Decreasing compliance in a regulated sector can be a sign of impending doom or at least sanctions from ambitious regulators. Benchmarking against others in the same line of business can serve as a useful KRI. If your organization is slipping from the middle of the pack toward the bottom, the likelihood of regulatory action increases.

Example Security Metric 15.5

Historic consequences of noncompliance	P	R	A	G	M	A	T	I	C	Score
	70	80	72	82	80	80	20	67	65	68%

Historical trends generally indicate systematic information security issues or common factors, providing information to help us refocus on achieving compliance where necessary. Considering this metric presents management with an opportunity to decide whether sufficient resources are being applied to security compliance activities relative to the myriad other things the organization needs to do.

* There is mounting pressure, in a few industry sectors anyway, for organizations to comply with the good practices in ISO27k, ITIL, etc. In some cases (such as PCI-DSS), the compliance requirement is imposed contractually. Sometimes certified compliance with ISO/IEC 27001 is *required* as a condition of doing business, and if the customer has enough clout (e.g., governments, major manufacturers, defense), there is little alternative: suppliers either implement ISMSs and get them certified or lose the business. Compliance metrics in this context have a very obvious and direct business value.

Tip: Audits, reviews, and assessments don't always generate scores or numbers: many just describe things in words. Where provided, ratings (even something as crude as red/amber/green) may provide useful data, but in most cases, someone will have to work through the reports diligently to generate meaningful metrics. Audit reports and possibly individual findings and recommendations, for example, can usefully be categorized and counted according to their significance (e.g., minor, moderate, or severe) or by subject areas, departments, etc., depending on the nature of the metric desired.

Example Security Metric 15.6

Number of systems whose security has been accredited	P	R	A	G	M	A	T	I	C	Score
	72	79	73	89	68	32	22	89	88	68%

{Metric 15.6} exemplifies the kinds of security metrics used in strongly hierarchical organizations. “Accredited” implies a process for assessing and accrediting (actually, certifying) IT systems against security configuration standards or regulations.

Example Security Metric 15.7

Status of compliance with internally mandated (corporate) information security requirements	P	R	A	G	M	A	T	I	C	Score
	75	75	73	63	65	58	40	40	70	62%

The organization, through its management, mandates a range of information security requirements that are largely documented in the form of policies, procedures, standards, agreements, etc., albeit supplemented by direct instructions, duties, roles, and responsibilities. Compliance with these can be measured in the same way as for externally imposed obligations. Noncompliance generally implies increased information security risks, but there may be legitimate, justifiable exceptions, and in some cases, noncompliance can be traced back to poorly expressed requirements. The metric needs to be interpreted correctly in order to action it appropriately.

Example Security Metric 15.8

Number of unapproved/unlicensed software installations identified on corporate IT equipment	P	R	A	G	M	A	T	I	C	Score
	58	55	82	73	86	47	64	66	17	61%

There is a potentially interesting distinction in this example metric between unapproved and unlicensed software. Approval concerns internal management authorization to install and use the software, whereas licensing concerns the legal right to copy and use it.

Being a simple count, this metric doesn't need much explanation to be Meaningful. It suffers because of the Cost of identifying and assessing all the software installations on all the corporate IT equipment—trust us, software auditing is a tedious, painstaking, and expensive task, one that is universally unpopular, except perhaps with software vendors (who, sensibly enough, outsource the actual work).

Example Security Metric 15.9

Percentage of security policies supported by adequate compliance activities	P	R	A	G	M	A	T	I	C	Score
	96	92	78	40	75	33	60	34	30	60%

Wouldn't it be nice if all policies incorporated or were accompanied by documented compliance processes? Even better, if they clarified the compliance responsibilities and allocated them to specific individuals! In a perfect world, corporate policies would specify compliance measures and metrics, forcing policy authors to think this through and, we hope, stopping them from mandating policies that cannot be enforced or their compliance readily measured.

Coming back down to earth, we have scored {metric 15.9} down on Genuineness, Accuracy, and Integrity as a result of that innocuous little word, "adequate," quietly minding its own business in the metric's name. The adequacy or inadequacy of compliance activities differ with each policy, for sure, and often differ between individual policy statements as well as their applications. Measuring and reporting compliance adequacy risks becoming the Nightmare Metrics Task From Hell

Tip: If recipients spend more time discussing or arguing about the precise meaning and wording of the metric than the data/information being reported, the metric isn't earning its keep. When selecting security metrics, it pays to think things through. Imagine yourself proudly presenting and discussing the metric to a group. Picture the kind of reaction it will create, particularly if it puts certain powerful managers in the audience under the unwelcome glare of the spotlight for their poor showing in the metrics tables and graphs on the screen. We're not advising you to avoid presenting awkward or unwelcome news necessarily; rather, pick your battles wisely. Metrics that put a positive spin on security and avoid emotive words tend to work out best in our experience, but we accept that not all metrics fit the ideal.

240 ■ PRAGMATIC Security Metrics

because of a million discrepancies and disagreements over what constitutes adequate compliance. That fraught discussion leads, in turn, to disputes about what exactly is meant by security policies, and, at this point, it's patently obvious to all that the metric is generating far more heat than light.

Example Security Metric 15.10

Compliance benchmark against peers	<i>P</i>	<i>R</i>	<i>A</i>	<i>G</i>	<i>M</i>	<i>A</i>	<i>T</i>	<i>I</i>	<i>C</i>	Score
	80	65	62	61	90	60	22	65	10	57%

In regulated sectors, an organization's compliance status may be judged and, to an extent, actively managed relative to its industry peers in the hope that the regulator may turn a blind eye to minor infractions and focus instead on frying bigger fish elsewhere. Benchmarking can also be indicative of the relative cost effectiveness of the organization's information security. Benchmarking studies are not cheap, however, and the sensitivity of information security makes it awkward to share information with peers, especially direct competitors. The cost is lower if comparative reports are readily available, for example, published surveys or reports from industry associations and groups, such as the Information Security Forum. Certified compliance with standards, such as ISO/IEC 27001, suggests an alternative, inexpensive approach: because organizations pay for the compliance assessments themselves and publish the key results (the certificates and, often, additional details, such as the scope of assessment or statements of applicability), tracking and reporting which of your competitors is certified would be a rather low-cost metric.

Example Security Metric 15.11

Number or rate of security policy noncompliance infractions detected	<i>P</i>	<i>R</i>	<i>A</i>	<i>G</i>	<i>M</i>	<i>A</i>	<i>T</i>	<i>I</i>	<i>C</i>	Score
	55	64	75	50	68	34	59	76	33	57%

Depending on how it is interpreted and used, {metric 15.11} could be either a compliance metric or a noncompliance-detection metric.* The underlying difficulties and expense of identifying noncompliance infractions (whatever that actually means) depress the Cost and Accuracy scores.

Example Security Metric 15.12

Embarrassment factor	<i>P</i>	<i>R</i>	<i>A</i>	<i>G</i>	<i>M</i>	<i>A</i>	<i>T</i>	<i>I</i>	<i>C</i>	Score
	26	38	20	50	63	72	40	87	87	54%

* If you don't specify it properly and use it consistently, it may end up being a Schrödinger metric—simultaneously both and neither.

Tip: Despite the disappointing absolute PRAGMATIC score, this example metric may still be of interest for the measurement system if it scores *relatively* well compared to alternative measures. That's another way of saying it may be the best of a bad bunch. For this reason, it is inappropriate to state categorically that any metric scoring less than *X%* will be discarded or that every metric scoring more than *Y%* will be adopted. Information security metrics is a tad more involved than that!

We assume the rather cryptic title of this metric is an attempt to measure the corporate embarrassment or outrage caused by a public incident, such as a serious privacy violation—maybe a credit card or customer database exposure. Incidents of this nature typically impact the corporation by discrediting it, harming its reputation, and devaluing its brands. If the public reaction is misjudged and the situation mishandled, things can blow up out of all proportion in a matter of minutes, thanks largely to online social media and instant global communications, turning an event into a crisis into a public relations disaster.

The metric's low **Predictability**, **Relevance**, **Actionability**, and **Timeliness** scores reflect the fact that by the time such an incident has exploded across the news headlines, it's largely beyond the remit of information security management. The internal incident management, forensics, and corrective actions quietly proceed behind the scenes to address the actual breach, but practically all the action relevant to the metric happens in the press office, on Twitter, and, often, on the CEO's doorstep.

On a rather different tack, who has been sanctioned for or embarrassed by noncompliance or incidents, and what were the actual business consequences? Gathering information of that nature involves trawling laboriously through news reports, press releases, industry rags, and Google searches, and then following up with the organizations and individuals concerned regarding the true costs (which most consider confidential). Rumors concerning major compliance incidents tend to circulate rapidly in most industries, but they are not necessarily reliable sources. Still, gathering the information may be worth the effort if it can be used subsequently to spice up security reports, awareness activities, training courses, case studies, and business cases for security investments.

Tip: There is something strangely captivating about being able to state, categorically, that "The lost backup tape incident last year cost the company \$2 million through fines and adverse publicity, carved 15% off the stock price, led to the resignation of the CIO and three senior IT managers, and set the security program back by 12 months." Those hard facts look an awful lot like metrics to us.

Tip: Costly metrics may be justified for occasional, ad hoc, or specific purposes but need to generate enough value to more than offset their Cost in order to be worth reporting regularly. Metrics can be cost–benefit analyzed, and value optimized, like most other activities.

Example Security Metric 15.13

Percentage of purchased software that is unauthorized	P	R	A	G	M	A	T	I	C	Score
	71	51	90	75	82	35	13	20	6	49%

Er, so we are presumably intending to check laboriously through the purchasing records (and maybe expense claims too, for good measure) and reconcile software purchases against some form of authority to purchase, then calculate and report the proportion? What exactly are we hoping to achieve with this metric? It may conceivably have a purpose in justifying a project to sort out the mess and fix a badly broken software procurement process, but what if the metric shows a rather low proportion of unauthorized software? The high Cost of the metric suggests we would probably be better off addressing the issues as we find them, rather than counting and reporting them.

Example Security Metric 15.14

Proportionality of expenditure on assurance versus potential impact × likelihood	P	R	A	G	M	A	T	I	C	Score
	65	40	85	40	3	20	46	76	35	46%

If only we knew what this metric was getting at, we might be able to explain it to management! What is meant by “proportionality” for starters? Reading gingerly between the lines, we figure this metric is probably aimed at measuring the appropriateness of assurance expenditure by determining whether assurance activities

Tip: If we had the energy, we should have made the effort to analyze the metrics requirement further and either rephrase or totally rebuild the metric, maybe brainstorming in a metrics workshop. Calculating their PRAGMATIC scores would be a rational way to compare and choose between variant or derivative metrics, perhaps using a pilot study to finalize the selection from a short list and refine the precise wording.

reflect risks. The vague and confusing wording in this case means the metric is probably dead in the water unless we have no better way to fulfill the metrics requirement (which is rather doubtful).

Example Security Metric 15.15

Proportion of software licenses purchased and not accounted for in repository	P	R	A	G	M	A	T	I	C	Score
	1	1	90	84	1	70	50	81	30	45%

ISACA presumably suggests this metric because purchased but unused software licenses are an unnecessary expense. If so, it is a rather narrow, highly specific metric. Arguably the metric is **Predictive** of an amount of money being wasted, but we really can't see any **Predictive** value or **Relevance** to information security; hence, it has almost no **Meaning** for information security.

Example Security Metric 15.16

Percentage of critical information assets residing on fully compliant systems	P	R	A	G	M	A	T	I	C	Score
	48	26	36	41	56	13	19	46	12	33%

The PRAGMATIC rating for our final metrics example suffers on two counts.

First, it refers to critical information assets, implying not only that someone has unambiguously identified them (which is a tall order but is a worthwhile activity with a number of business continuity and other security benefits, besides better metrics) but that management fully appreciates and accepts the meaning of critical information assets. We suspect we would end up having to explain and discuss the phrase repeatedly if we went ahead with a metric like this, taking valuable management time and head space away from considering what the metric is actually telling us. It's an unfortunate distraction.

Second, there's the issue of fully compliant systems. Compliant to what? "Fully" emphasizes that compliance is an analogue rather than binary value—fair enough—but who determines how full is "fully" and on what basis? Checking multiple technical configurations in enough detail to confirm whether the systems are

Tip: "Fully compliant" also has a nasty sting in the tail if it is naïvely interpreted or understood to mean "fully secure." Be very careful to distinguish compliance requirements from good security practices.

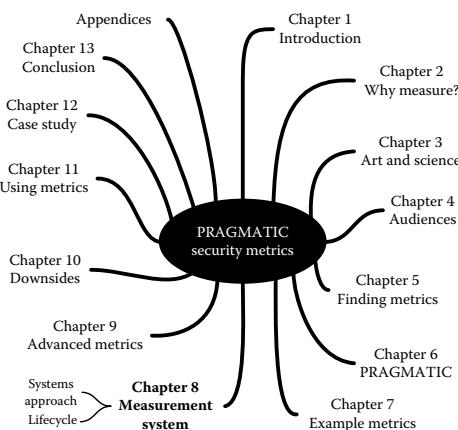
fully compliant is a time-consuming exercise unless the configuration standards are trivial, which seems doubtful in the kind of organization where this metric would make sense. Low Accuracy, Cost, and Timeliness scores take their toll, so this metric is unlikely to make it off the drawing board.

7.13 Summary

This chapter, the longest one in the book, described the factors that led us to PRAGMATIC-score more than 150 information security metrics examples. Many of these metrics have been collected from a variety of published sources in addition to those we have contributed ourselves. Our objective was to provide a wide range to illustrate the relevance of using the PRAGMATIC process to select the best and weed out the worst. Structuring the metrics in line with ISO/IEC 27002 makes the chapter particularly helpful for organizations with ISO27k-compliant information security management systems, but the principles are universal. Along the way, we introduced a novel process maturity measurement and hammered home the point that security metrics range on a continuum from very good to very poor, the PRAGMATIC method providing a systematic and rational way to assess and compare metrics.

Chapter 8

Designing PRAGMATIC Security Measurement System



Devoting sufficient time to establishing information security performance measures is critical to deriving the maximum value from measuring information security performance.

NIST SP800-55 revision 1 (NIST 2008)

Tip: This is a challenging chapter. If your head is spinning already, take a break at this point to let things sink in. Go back over your notes, maybe, and carry on practicing the PRAGMATIC stuff. There is no rush—it can wait.

OK, we have somehow found the time to devote to security metrics. We have walked through a structured process for specifying and scoring a single metric, and we've practiced our skills on 150+ metrics examples. But how, exactly, do we establish performance measures that will derive maximum value from information security? We have a way to go yet.

In this chapter, we'll be bringing the ingredients together as a coherent whole, consciously selecting metrics that complement and support each other as elements of an *information security measurement system** with business value above and beyond the accumulated value of the individual metrics.

8.1 Brief History of Information Security Metrics

Before we continue, we feel the need to remind ourselves of the context.

Prior to the 1980s, data security barely existed as a practice area, let alone a professional field of endeavor outside of the military and intelligence agencies where many of the still-current issues had been worked on since the mid-1960s. Most of the commercial security effort back then went into managing user IDs on mainframes, minis, and shared servers (apart from a swelling rank of hobbyist/homebrewed machines, there were no personal computers). Access rights within applications were generally binary (privileged or not). There were few security products on sale other than security subsystems for the mainframe systems and consultancy services. Backups were performed by backup operators. Business continuity didn't seem to be much of an issue, and there were hardly any laws and regulations concerning data security or privacy. Hackers were actively developing exciting new technologies. There was nothing much to measure, hence no security metrics.

IT security sprang up during the 1980s along with the market for security products, such as rudimentary firewalls (for corporations) and antivirus software (for the exploding market in PCs). It was possible to make a living from security as a result of growing demand from the financial services sector in particular. Hackers were actively exploring networks and telephone systems. Introduction of the quality assurance standard BS 5750 by British Standards in 1979[†] started to influence busi-

* While it is tempting to use the abbreviation ISMS, we don't want to confuse you with information security management systems.

[†] Later becoming ISO 9000.

ness management with an upsurge of interest in the concept of business *processes* and process controls, including business metrics. A few organizations introduced basic security metrics but, without much of a clue what to measure or why, they tended to measure the things that were easy to measure rather than worth measuring.

In the 1990s, professionals started to specialize within security (e.g., security architects and network security analysts), and the security jobs market expanded across all sectors. Viruses became headline news, and underground hacker clubs took off. The concept of information as opposed to IT security slowly emerged, leading to the creation of information security manager roles in most large companies. In 1995, BS 7799* introduced quality assurance and process control practices to information security, and the process view of security gradually emerged as it became all too apparent that merely owning a firewall was not sufficient to be secure: it had to be installed, configured, and managed correctly. Security metrics around this time seemed to be driven mostly by the provision of reporting functions within systems and security products. We saw our first security consoles, often associated with moves to centralize security management and get some control of the disparate range of security technologies rapidly spreading across corporations.

From about 2000, we have seen the growth of governance and (especially post-9/11) ever-increasing concerns about information security risks, leading some organizations to create even more senior roles (such as CISO) to ensure that information security receives sufficient management attention. The involvement of organized gangs has seen hackers become crackers become criminals: the stakes are much higher now, especially given that virtually all systems are now either directly connected to the Internet or just one or two hops away. Throughout the 2000s, management information concerning the state of security has grown increasingly important, driven to a significant extent by the imposition of governance, information security, and privacy-related laws and regulations, not to mention the milestone level of internet fraud and general crookery achieved last year as it globally headed north of *\$1 trillion*. Today's substantial security compliance burden means management can no longer afford to leave it to the techs—they need assurance that key security risks are truly in hand. Security metrics specialists began writing books and articles, raising awareness (mostly, it has to be said, within the information security profession) of the possibility of providing worthwhile management information through security metrics.

Today, we face a growing demand for good security metrics from information security managers, CISOs, auditors, regulators, and business people generally. A number of standards projects, special interest groups, and metrics experts have attempted to bring some order to the field during the past 5 to 10 years but have achieved little consensus on which security metrics are good and, by implication, which are bad.

* Later becoming first ISO/IEC 17799 and then ISO/IEC 2002.

Tip: Because you have read this far, you clearly have a genuine interest in the subject, so you may already be familiar with some of the other books, standards, and papers on security metrics. The Bibliography in Appendix L is more than just a set of references: it's a suggested reading list.

Information security is a dynamic field because the risks fluctuate in a complex and, hence, not entirely predictable manner. Cloud computing and BYOD* are two hot security topics as we write this: there will undoubtedly be others by the time you read this book. The way organizations use and depend on information security is also changing: over time, growing confidence in security controls and metrics tends to lead to decay in the checks and balances that are seen as superfluous and unnecessary. Looking forward, we see the potential for nasty surprises in store for managers who believe, partly on the basis of their security metrics, that their risks are entirely under control. Information security may be, but the risks are another matter entirely.

8.2 Taking Systems Approach to Metrics

Newcomers to the field tend to contemplate individual security metrics in isolation, and, to be fair, up to this point, we haven't gone much further: having rated a given metric using the PRAGMATIC criteria, we can, of course, use the score to compare or rank it relative to others, but, despite being a significant step, that's about it.

We move on now to discuss a more coherent approach to using metrics in the context of business and security management that involves designing, implementing, using, and managing an *information security measurement system*. A comprehensive system will encompass all aspects of measurement relevant to managing information security, leaving no significant gaps and limiting the overlaps to areas that deserve the additional assurance of cross-checks and alternative perspectives.

Worthwhile *information security measurement systems* don't magically pop into existence of their own accord: they have to be conceived, controlled, and actively managed in order to meet the organization's need for information supporting all the information security and risk management decisions that are required. We'll lay out the process for designing and implementing your *information security measurement system* shortly.

* Bring Your Own Device—employees using their personally owned IT devices for work purposes.

8.3 Information Security Measurement System Lifecycle

The structured project management lifecycle approaches* normally applied to software developments and other engineering initiatives can usefully be applied to measurement systems, too. Doing so empowers us to control and direct the process, making sure key activities and stage gates (key control points) aren't simply skipped, bypassed, or omitted. Lifecycles vary in detail, but the overall sequence[†] and key stages are generally along the lines shown in Figure 8.1.

Phase 1: Requirements Specification

Phase 1 involves gaining a solid appreciation of the organization's information security-related information needs (i.e., the requirements both for the metrics and for the measurement system) by persuading your respective security metrics audiences to consider, discuss, and document, if not formally specify, their strategic, tactical, and operational objectives relating to information security management, controls, risk management, and governance.[‡]

As with software development and other engineering activities, specification is arguably *the* most important phase of the lifecycle, yet it is perhaps the least well understood and followed in practice.

We need to figure out why we are measuring information security, what aspects—specifically—we are trying to measure, who will act on the measures, and how they define success.

If you don't know which way you are headed, any route will do.

Information security is notoriously difficult to measure, the main issues being, first, how to measure risk itself and, second, how to measure the reduction in risk as a result of information security controls, in particular, the anticipated decrease in the number and severity of security incidents. That's primarily what we're trying to achieve through information security, although there are other reasons and benefits (such as for compliance with external obligations, to assure management and other stakeholders, or to enable business activities that would otherwise be too risky to pursue).

* It could also be said that individual metrics have a cradle-to-grave lifecycle: they are conceived, and they gradually mature (some of them becoming valuable sources of important management information) until eventually they run out of puff and are replaced by the next generation of metrics. The *information security measurement system* provides a management framework, a set of processes or tools with which to direct and control the lifecycle of individual metrics, including contraception and euthanasia.

[†] Despite the nice clean arrows clearly implying a defined sequence of stages, real life is never quite as tidy as the theory suggests. In practice, there is usually a fair amount of hesitation and repetition (iteration). Deal with it.

[‡] Regardless of the metrics context, that's an excellent goal in itself!

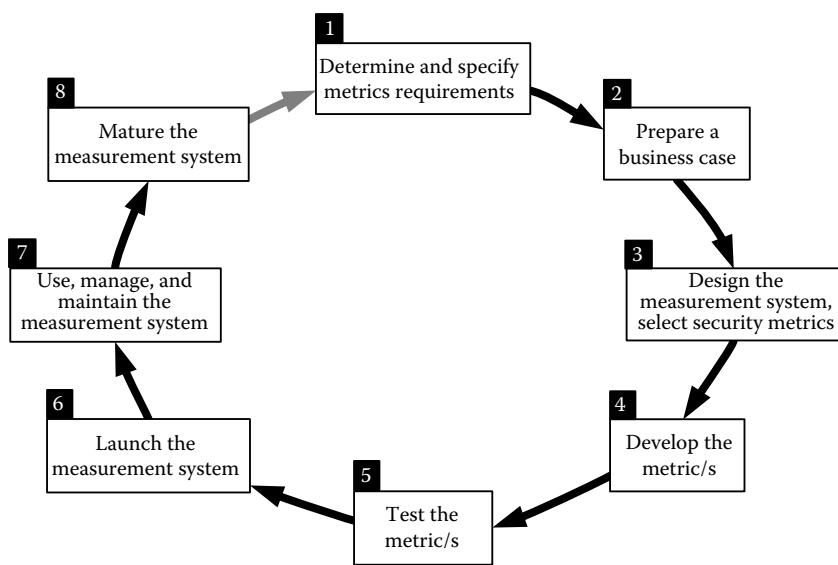


Figure 8.1 Information security measurement system lifecycle.

We might perhaps measure and track the number and severity of information security incidents in order to prove to management that they were wise to have invested in an information security management system or security improvement program. If the number and severity of incidents fall, we would probably claim the security effort has been a resounding success, but if we are honest, it is possible that we are simply seeing a random effect: perhaps the threats have fallen, or the threat agents have been busy elsewhere and may yet return. Conversely, if the incidents increase, that does not necessarily mean our controls are ineffective: it could be that the risks have increased—perhaps more vulnerabilities are being exploited on the IT systems we use.

The real issue is one of conjecture. It is impossible to measure objectively what *might* have happened as a result of incidents *if* we had not implemented or improved our information security controls.*

Nevertheless, it takes an unbridled optimist to contend that information security risks are entirely trivial or inconsequential. Doing nothing is an untenable position for management given that so many organizations suffer serious security incidents every year, some to the point of ceasing to exist.

Phase 2: Business Case

Phase 2 involves justifying the *investment* in the *information security measurement system* on the basis of its projected business benefits and gaining management

* Trying to *prove* a negative, typically the absence of something, is tough: ask any atheist.

Tip: When developing application systems, prototypes usually help the eventual users picture themselves in the driver's seat. A mock-up management report or metrics dashboard may be just the ticket to persuade management to think in more depth about their needs and elaborate on the requirements (their metrics goals and anti-goals). The trick to a good prototype is to maintain focus, keeping management's attention on what they foresee in the way of useful information content, rather than the form of its presentation at this stage. Don't, whatever you do, make your prototype too glossy, polished, and credible or they will demand it, *right now!*

approval. The business case is arguably the most important document for the implementation project.

We've said before that commercial organizations are run by the numbers, most obviously those big headline figures with dollar signs attached (income, expenditure, profit, price/earnings ratio, etc.), but in reality, there are numbers on almost everything (production numbers, defect numbers, customer numbers, etc.) except, it seems, for information security. In the past, we simply haven't had credible, meaningful numbers to present.

Business cases within any one organization are generally based on a standard template in order that management gets familiar with the structure, layout, style, and content. Although there is no universal standard, a typical business case includes the following:

- Executive summary—the crucial details expressed in a paragraph or two
- Title, date, author, version, and status—document control information
- Introduction, background, context
- Clear statement of the problem to be addressed, including the scope—the justification for the solution
- Proposed approach, often stating any alternatives considered and possibly discussing other options

Tip: The proposal to develop and implement an *information security measurement system* is itself an excellent way to demonstrate that information security is amenable to being measured. We recommend developing a sound business case, even if the investment is relatively small, so a business case may not strictly be required. Consider it an awareness activity, an opportunity to sell the idea of better security metrics to management.

- Anticipated outcomes and deliverables
- The value proposition—a financial analysis of the projected costs and benefits using NPV, IRR, etc., possibly with confidence limits and contingencies
- Key assumptions or constraints, plus risks and dependencies, often including CSFs, KGIs, and/or KPIs (see next chapter)
- High-level project plan, at least the key dates or timescales
- Project governance information, for example, stakeholders, project manager, project control board composition

One of several important issues to clarify for the business case is the scope of the *information security measurement system*. As with any other system, it will comprise a set of in-scope metrics and measurement processes that are to be managed separately from, but perhaps interfacing to, other out-of-scope metrics and measurement processes. Other management disciplines have their own measures, metrics, and, in some cases, perhaps even what might be termed measurement systems. Here are some examples:

- *Financial metrics*: almost anything containing a dollar sign is a financial metric, but the most significant figures really catch management's beady eye.
- *Operations/production metrics*: measurements and statistics relating to production processes and shop-floor machinery.
- *HR or personnel metrics*: number of employees/contractors/consultants/tempers and so forth.
- *Health and safety metrics*: "Days since the last lost-time accident" is a typical metric mentioned elsewhere in this book.
- *Risk and risk-management metrics*: these may reflect the blinkered SOX approach to life, or they may extend beyond SOX-relevant systems to encompass a broader variety of strategic and operational risks, including those that fall outside the organization's boundary (e.g., supply chain risks) plus the processes used to identify and respond to risks.
- *Compliance metrics*: legal and regulatory compliance is undeniably driving a lot of management controls, but the issues here are much broader in fact. Noncompliance with national and international standards, plus internal strategies, policies, and procedures, may not land the CEO in jail but can certainly harm business interests. Again, both the compliance status and processes can be measured.

Scoping is the process of defining the boundaries and reducing, as far as practicable, areas of both overlaps and gaps. It involves clarifying which, if any, of those metrics or types of metrics will be managed within the *information security management system*, aside from the pure information security management metrics that are definitely in-scope.

Tip: Be *very* careful about the scope. When* the *information security measurement system* turns out to be wildly successful, management will naturally want to extend the winning formula to other management information and metrics. They may wisely choose to establish a number of distinct but interoperable measurement systems, perhaps all modelled in the same way, using their own PRAGMATIC metrics. If, however, they simply start to extend the *information security measurement system* to incorporate first related and then less-related metrics...well...you can see where this is headed. We recommend defining the scope as explicitly as you can and then proactively managing any changes.[†]

* Not *if!* Remember, the business case has to sell the concept to management, convincing them to invest in the *information security measurement system* specifically and generally take more of an interest in security metrics. Being positive and upbeat, and discussing it enthusiastically will help your cause. Well, it won't hurt.

[†] Far from being shoved away in the bottom drawer once it is approved, every business case should be treated as a living document, actively maintained and change-controlled. For instance, if the project is rescoped, this inevitably changes the likely benefits as well as the costs.

The heart of any business case is the value proposition laying out the net value* of the investment in financial terms. If the core value proposition isn't sufficiently convincing, the proposal is far less likely to get a buy-in from management. So what are the costs and benefits of an *information security measurement system*?

First, elaborate on the costs. We suggest dividing the costs into two distinct categories:

1. Costs associated with the implementation project—for example, the man-hours needed to determine the initial metrics requirements, run workshops, PRAGMATIC scores, etc., and to manage the project.
2. Cost associated with the *information security measurement system* itself once it is up and running. While a few information security metrics may be based on raw data that are for all intents and purposes free (e.g., readily available data already being collected for other purposes), most will require technical systems and processes to be instrumented in some manner to generate

* Net value is the benefit derived from the investment less the investment cost. Note that the benefit can involve new/additional income and reduced/avoided expenditure—the dollars are equally valuable either way.

Tip: In addition to the costs of conventional project management/project control group meetings to guide the project, why not also specify in the business case quarterly senior management meetings to consider and respond to key information security metrics? Estimate the meeting costs rationally (so many senior-manager-hours at their nominal rate). By doing so, when the business case is approved by senior management, they are in effect agreeing to participate in your quarterly metrics meetings.

the raw data, implying expenditure there.* Furthermore, *all* metrics have to be analyzed, presented, and used, and the system will need to be managed, incurring costs there too.[†] You won't have all the figures yet, so estimate.

The reason for splitting them up is that the project will come to an end at some point, but there will be recurring costs associated with the system throughout its lifetime.

Estimate the costs on the generous side, add them up, and then add some contingency on top to allow for unplanned additional expenses and overruns if the project risks turn out to have been inadequately controlled.

Next, the benefits.[‡] You are going to have to get creative here because the financial benefits mostly depend on the nature of the metrics that have not yet been chosen! There are many clues about the potential business benefits throughout this book, particularly in terms of gaining answers to the rhetorical questions posed way back in Chapter 2. For example, with a reasonably comprehensive set of PRAGMATIC security metrics, management will be able to do the following:

- Manage information security at least partly by the numbers, giving efficiency savings
- Make the organization more secure, cutting the probability and impacts of security incidents

* If you need a refresher, go back for another look at the Cost criterion at the end of Section 6.3.

[†] A canny information security manager is glad to offload ownership and Costs of peripheral information security metrics onto other corporate functions in order to focus his or her attention and resources on core security metrics that are crucial to information security management. Regardless of where ownership ends up, actively collaborating with other functions on metrics that span organizational boundaries and responsibilities is a vital part of the job.

[‡] Figuring out the projected business benefits in some detail will be particularly worthwhile when it comes to determining and optimizing the net result later on. The benefits are a key parameter for the business case and drive the project as well as becoming key metrics for the *information security measurement system* once it is operational (this is the essence of the Val IT approach to more cost effective IT project management—see ITGI (2008b) and Thorp (1998)).

Tip: Keep the business case overtly business-oriented. Discuss the benefits in terms of how better security makes things better (safer, cheaper, less risky, more confident) for the business and for management, rather than positioning better security as an end in itself.*

* Advertising professionals talk about selling the ability to fix stuff, not the nails. Car ads do it all the time, selling the lifestyle, freedom, and excitement, not the lifeless bits of steel, plastic, and rubber sitting on the tarmac. Perfume ads sell the glamour and allure, not the smell (“fragrance” being the preferred term). The time-worn rubric of “sell the sizzle, not the steak” pertains here. Get it?

- Increase operational predictability and avoid ruinous surprises—big pluses in driving positive share value itself of keen interest to management holding stock options
- Gain a better understanding of information security risks and be able to direct security resources from less risky toward more risky areas, thereby optimizing resource allocations (e.g., avoiding investments in unnecessary controls)
- Identify and start dealing with emerging security issues, compliance obligations, etc., earlier, leaving more options open and just possibly getting off the crisis du jour, reactive, fire-fighting mode of operation
- Gain more assurance/certainty as to the organization’s security status, facilitating business initiatives that might otherwise be too risky
- Offer credible fact-backed assurance to regulators, business partners, and other stakeholders on the organization’s security status

The business case should be comprehensive (providing sufficient information for management to make a rational decision) but must remain comprehensible (make sure it is clearly written and well structured). The numbers presented must be transparent; that is, you must be able to substantiate them, but it is OK to put the supporting details and explanation for the basis of your estimates in appendices, leaving just the key figures up front.

Phase 3: Design

Phase 3 is about designing the *information security measurement system*, applying conventional architectural methods/approaches in this context. In this phase, we select a coherent suite of PRAGMATIC security metrics with each chosen metric having a vital part to play and contributing to the entire measurement *system*. Keep in mind that some metrics may warrant selection because they support or cross-reference others or fill a critical gap in the system even if they don’t score particularly well on the PRAGMATIC scale.

The business model for information security (BMIS—see Appendix B) points out that information security benefits from a systems approach that involves “understanding the interrelationships between the parts of the system such as people, processes and technologies and how changes in any one element inevitably causes changes in others. The essence of systems theory is that a system needs to be viewed holistically—not merely as a sum of its parts—to be accurately understood. A holistic approach examines the system as a complete functioning unit. Another tenet of systems theory is that one part of the system enables understanding of other parts of the system. ‘Systems thinking’ is a widely recognized term that refers to the examination of how systems interact, how complex systems work” (ISACA 2009).

The *information security measurement system* design process takes into account how the metrics will interact both within and without the measurement system, for instance, how they complement each other plus metrics used in other business functions (see Section 5.2). There may be synergies with other departments, perhaps opportunities to share base data or marginally extend existing analytical and reporting processes to the benefit of security or to use security metrics to inform decision making within various business processes. The information security metrics need to fit into and support the wider context of the organization’s overall management practices, positioning security measurements as an integral part of governance and management practices alongside financial metrics, operational metrics, and all other forms of management information. In mature organizations that routinely use a plethora of metrics to manage by the numbers, the information security metrics must dovetail with other related metrics, such as those relating to information management, risk management, compliance management, and so forth.

Take, for example, metrics relating to the governance of information security: this is a subset of corporate governance (Figure 8.2), and hence, there may already be corporate governance metrics that can and ideally should be applied

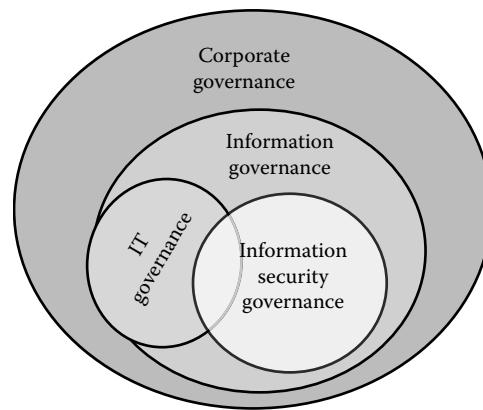


Figure 8.2 Governance relationships.

to information security. If, however, the organization lacks much in the way of governance metrics, those proposed for measuring and managing the governance of information security may have wider interest or application that might warrant highlighting.

As the development of the security measurement system proceeds and key aspects of the design crystallize out from what tend to be rather vague and uncertain origins, an overall metrics architecture may emerge naturally or it may be consciously elaborated and developed as part of the process. There are clear parallels here with software or IT systems development processes: the measurement system can be designed introspectively and narrowly, but taking a broader enterprise-wide or strategic perspective will probably pay dividends in the long run.

Part of the architectural design process involves avoiding unnecessary duplication or overlaps between metrics while, at the same time, avoiding serious gaps. In other words, rather than measure the same aspect of the same thing multiple times, measure other relevant or complementary aspects to generate valuable new information, and when possible, provide a cross-check on the validity of the other metrics.

Identifying candidate information security metrics for the *information security measurement system* is an interesting exercise. Having worked through the example metrics in the previous chapter, you probably have a number of possibilities in mind already. The organization may be using some information security metrics,*

Tip: This is where your metrics catalog comes into its own. In the unlikely event that you aren't already keeping some sort of list of interesting information security metrics, start now. As a tool, it will support the *information security measurement system* and will be invaluable when specifying, scoring, considering, choosing, and maintaining your metrics. It will be a place to keep the PRAGMATIC ratings and those notes we've mentioned several times, and you will need fields for all the important parameters/specifications. Unless database design happens to be your forte, get some help with this. It is not unusual to end up with literally *hundreds* of information security metrics in the catalog, though we hope only a fraction of them are actually in use at any one time.*

* For the limited purposes of writing the book, we settled on a minimalist database, namely, a spreadsheet. If your resources are tight to nonexistent, a spreadsheet may suffice for a while until the measurement system has proven its worth anyway. Aside from being cheap, it is a flexible way to figure out your requirements.

* Project metrics relating to information security initiatives, for example, or to information security activities in software development and business change projects.

and hunting through management reports will probably reveal others that are not necessarily thought of as security metrics: provided they are relevant, existing, familiar metrics should be considered and scored alongside new ones. Taking account of management information needs elaborated in phase 1, draw on reference sources, such as those noted in Chapter 5 and in the bibliography (Appendix L), for inspiration on additional candidate metrics, using brainstorming and similar creative thinking and teamworking approaches to come up with novel approaches as well as to review and refine earlier suggestions.

The main activity in phase 3 is short listing metrics, which involves using the PRAGMATIC method (described in Section 6.4 and illustrated more than 150 times in Chapter 7!) to score the candidate metrics individually, and then selecting suitable metrics from the ranked list.* Ideally, both activities, particularly the selection part, should involve management directly, although you might help things along a bit by highlighting or preselecting the most obvious candidates.

Two complementary ways of selecting metrics are as follows:

1. *According to the measurement requirements:* starting with a clear idea of the management objectives of information security, pick out metrics from the catalog that meet the measurement requirements stated in phase 1 of the project.
2. *According to the availability of candidate metrics:* look through the catalog for potentially worthwhile metrics.

Either way, we recommend using the PRAGMATIC scores and notes to guide the selection process. However, it's best to select a class or category of metrics needed for each area deemed important to measure and then score each candidate metric in the group to find the best options for that category. An example would be the need to measure compliance. Because there are a number of metrics that might serve in that category, they should all be scored for best fit, form, and function, bearing in mind issues of interoperability and cross-referencing mentioned earlier. In other words, in the design phase, select categories of metrics, determine the candidate metrics, and then score them to find the best options.

Nobody can say definitively how many metrics to short list.[†] It should be pretty obvious at this stage when you have selected enough to be getting on with. You will pare down the short list still further in the next stage, but avoid the temptation to include too many variants or low-scoring metrics: now is a good time for

* Managers may express an interest in the PRAGMATIC scoring process and might query or challenge some of the assigned scores at this stage, but more likely, they will simply accept your list as presented and immediately start thinking about the metrics, particularly those toward the top of the list. Don't worry, this is a good sign!

[†] However, you *probably* don't want hundreds! You will soon start incurring costs to develop and test the metrics, so be realistic about how many you can sensibly handle, given your current state of metrics management maturity and the resources available for this.

Tip: Don't forget that metrics can be filtered according to their ratings against one or more of the individual PRAGMATIC criteria or by their assigned categories/types, for example, to identify strategic metrics that are relatively Predictive.* The PRAGMATIC scores are intended to support rather than constrain management decisions. There may be perfectly valid reasons for selecting a few low-scoring metrics—the operative word being “few.” There has to be a justifiable rationale for including them on the team. Be sure to take notes!

* Now do you see why we suggested getting help with the database design?

management to start making choices with the knowledge that the decisions can always be revisited later once the system is running.

Remember, the short listed metrics will be the building blocks for the *information security measurement system*. This is not unlike picking the members of a team. Rather than mechanistically selecting, say, the 30 top-scoring metrics, look out for complementary, mutually supportive metrics directly addressing the measurement requirements previously stated by management.*

Bear in mind that a given metric may serve a number of purposes, being relevant for a number of different people and purposes. For example, a lack of compliance in one specific area (such as failing to accompany visitors while on site) may indicate compliance issues elsewhere (perhaps reflecting a casual disregard for physical security among employees). This metric is likely to be of direct concern to the people in charge of physical/site security but may be of general interest to the training and compliance people or, indeed, may serve as a key risk indicator by tracking the trends.

For key information security metrics driving critical business decisions, management may require additional assurance that the measurements are sufficiently Accurate, Genuine, credible, and reliable. Considering possible failure modes may suggest ways in which metrics can be validated. For example, it may be appropriate in some circumstances deliberately to adopt complementary or overlapping measures in order to identify errors and highlight discrepancies between them. Although this increases gross costs, the additional assurance may make it worthwhile. We will explore this important aspect further in the next chapter.

Congratulations, you now have a working short list of PRAGMATIC information security metrics! Soon, you will refine the short list, fleshing out the practical details and probably making minor changes, but for now celebrate reaching a major milestone on your project.

* It helps immensely if there is a genuine management demand for the information. If proposing to drop certain metrics from the team creates serious misgivings, the demand is probably real.

Phase 4: Development

The *information security measurement system* really starts to take shape in phase 4 as you put in place the processes, data collection/feeds, data analysis, and presentation/reporting activities for the short listed metrics.*

Every metric has one or more sources of data. For metrics that utilize significant volumes of data, it generally makes sense to automate the data collection using data interfaces, file transfers, etc., provided it is cost-effective to do so. This may also be the time to consider possible ways of condensing or summarizing the data to render them more manageable. Conversely, for metrics that utilize relatively small amounts of data (normally quite simple measures reported infrequently), it tends to be most cost-effective to collect the data manually when required.[†]

Rather than collect the raw numbers and analyze them centrally, sometimes they are analyzed by the systems that generate them, significantly reducing the amount of data to be collected. However, this means you are reliant on the local data analysis. If the information is vital, the analytical processes should probably be checked, at least, and steps taken to ensure they are placed under change control to prevent inappropriate configuration changes.

Data collection can be periodic (usually hourly, daily, weekly, monthly, quarterly, or annually) or event-driven (e.g., collected when there are so many kilobytes or megabytes, when requested by the analytical system/process, or if certain conditions occur).

The analysis of data also varies a lot depending on what is to be reported. Some metrics consist of just counts or proportions; some involve simple calculations, such as means (possibly rolling means), and others involve more elaborate mathematics/statistics (e.g., finding correlations, outliers, or rates of change), sometimes combining multiple data sources.

Having casually mentioned processes a moment ago reminds us not to overlook the human beings who are expected to operate, use, and manage the *information security measurement system*. Procedural documentation generally helps clarify and standardize any complex or infrequent operations, including, for instance, what to do if a metric goes off the scale, delivers confusing or contradictory information, or fails.

Phase 5: Testing

Any complex machine needs to be exercised and proven, and the *information security measurement system* is no exception. The testing in phase 5 involves techniques,

* We have more to say on data collection analysis and reporting in Chapter 11.

[†] A slight complication arises in the case of data points that are only required infrequently or at indeterminate points, where there is a possibility that the raw data might be deleted or lost before the collection takes place. This can be handled through procedures (e.g., collecting the data routinely and storing them safely until analysis and reporting) or routine data archival. It's one of many small details to sort out in this phase.

Tip: Follow the KISS principle: keep it simple, statistically. Unless you were rigorous in the previous phase and short listed only a handful of metrics, you probably have a lot on your plate, especially given all the variations mentioned in this section (and we're barely scratching the surface here). Given the choice, start working on the most valuable metrics first: get them running, and start reaping the benefits.

such as prototyping, pilot studies, and trials, to check the metrics out and refine the analysis and presentation elements.

Checking the systems and processes used to collect, analyze, and present metrics in a safe, contained environment (such as a pilot study) helps confirm that they will work properly when rolled out for real. This is the ideal opportunity to gather feedback from users on whether their needs will be met (e.g., do the chosen metrics presentation formats resonate with the audiences?). This and all prior stages are iterative to an extent: we learn things in the course of specifying, designing, developing, and testing metrics and can refine the measurement system to some extent as we go.

Another less-obvious activity in phase 5 concerns the reliability of the metrics themselves. We have mentioned before that there are risks associated with metrics supporting critical security decisions. In the science and engineering sphere, specifications are prepared for the instruments and measurement processes for crucial measurements, laying down key characteristics, such as their accuracy, precision, repeatability, and reliability. Without going completely over the top, it is worth thinking about the quality and reliability of key metrics because the consequences of errors or failures may be serious. For example, if it is crucial that the logical access controls are working properly on a network carrying highly sensitive/valuable information, management may wish to monitor metrics relating to logical access attempts (perhaps the number of successes *and* failures in this case). In order to counteract the possibility of the measurement process failing (e.g., if a vital measurement system, interface, or network connection falls over or starts operating erratically), we might perhaps rig a test system that attempts to access network resources in various ways, confirming that the access attempts are accurately reflected in the metrics reports.

Tip: Writing good procedures involves making an effort to understand the processes and express them succinctly in straightforward terms. Think of this as a valuable extension of the specification phase, not just a tedious writing exercise. Use diagrams, such as flowcharts, to keep the interest up, augment comprehension, and keep word count down.

Tip: This is a similar concept to the display test function on the console of a complex machine. Pressing the test button sends electrical signals to the various subsystems, which respond by lighting their lights, showing full-scale deflections on the meters, and so on. The operator can tell at a glance if any subsystem does not respond correctly and so is defective. Modern computerized control systems are much more complicated, but much the same principle is still used. Pressing the button now sends computerized commands to the subsystems, triggering their self-check functions, or injects specially tagged test data that exercise the subsystems in a predictable manner.

Phase 6: Launch

It's time now to implement your information security metrics, and start using them in earnest.

The implementation and initial use of metrics can be handled as a change management activity:

- Plan ahead to avoid conflicting changes, including heavy-duty business activities such as end-of-year.
- Make sure users are ready to start using the metrics (e.g., do they need awareness or training materials outlining how the new metrics are intended to be used and explaining any user controls, such as configurable reporting parameters?).
- Take care if you are changing the basis of trends analysis (e.g., be prepared to restate prior periods).
- Verify that the implementation has worked properly (e.g., check with the users that the metrics meet their needs) and have a back-out plan in case it didn't (e.g., revert to earlier metrics—perhaps maintain original and new metrics in parallel for a trial period).

Phase 7: Operating, Managing, and Maintaining

Once the *information security measurement system* is implemented, it will settle into a routine. Typical activities in phase 7 include monitoring the system for issues and minor improvement opportunities, instigating the appropriate responses, and managing changes, including changes to the systems and business processes that are the source of the raw measurement data plus the networks, analytical systems, reporting systems, and processes.*

* See also Chapter 11.

Tip: There is no particular reason, apart perhaps from convention, to attempt to implement the entire *information security measurement system* in one go. There are often advantages, in fact, in deliberately staggering the introduction of new metrics, for instance, giving recipients time to get familiar with and start making use of one tranche of metrics before launching the next one. It's up to you how you define a tranche—groups of related metrics, perhaps, or the most important/valuable metrics first or, more prosaically, whichever metrics are ready to launch.

Another activity involves confirming that the measurement system and the metrics are actually generating the business benefits they were intended to achieve.

Considering first the overall system, the business case from phase 2 laid out the projected costs and benefits. Now that the system is operating, it's time to validate the assumptions and projections, confirming that the claimed benefits are on track. We're talking here about using metametrics, that is, information about the metrics, such as reviewing and responding to audience feedback.

Extending that thought, there are probably things you can do to squeeze more value from the individual metrics once they have settled down. At first, however, you will probably be more concerned with ensuring that they are operating as expected, the data collections, analyses, and reports are working correctly, the metrics audiences are happy with the information and are making good use of it, and ultimately, the metrics are driving various improvements to the organization's information security status.

The mere fact that good (i.e., PRAGMATIC) information security metrics are available where previously there were none will inevitably start driving organizational change. The axiom "that which gets measured gets done" is relevant here. Unflattering or, worse, damning metrics delivered at the right levels of the organization will cause a reaction that we hope leads to better behaviors and, hence, a desirable outcome. Unpalatable metrics may, of course, also lead to an unplanned career modification for the metrician.* Metrics portraying management decisions in an unfavorable light are unlikely to be welcomed by those managers as many of us

Tip: The Val IT approach (Thorp 1998; ITGI 2008b) goes beyond merely confirming the original projections, proactively using various controls built in to the system and its supporting processes to maximize the realization of business benefits.

* If you expect to receive honest and complete information in the future, don't shoot the bringer of bad tidings!

have witnessed. To be fair, in some organizations, such negative or adverse metrics are embraced as learning points that provide the basis for systematic improvements. Appreciating how information security metrics will be handled by the organization is one aspect of corporate culture the prudent information security manager (and others) should appreciate.

Phase 8: Maturing the Measurement System

Provided the change management and maintenance activities noted in phase 7 are operating correctly, the *information security measurement system* will naturally evolve and gradually mature under its own steam, in other words, without any specific direction or controlling actions. However, the evolutionary pace is slow and uncertain, so we recommend management getting together to review the system as a whole every year or two.

The kinds of things that may be worth doing in the *annual information security metrics workshop* include the following:

- Reviewing the information security metrics to ascertain whether they are effective and adequate, looking for opportunities to retire any that remain unsatisfactory (despite previous attempts to improve them) and introduce new PRAGMATIC metrics where justified, for example, to bolster areas that are poorly metricated (more below)
- Reconsidering the overall measurement system design/architecture, for example, automating more metrics, perhaps even linking up with other measurement systems
- Responding to the inevitable changes in the organization, its business environment, and, most of all, its need for information security metrics
- If appropriate, initiating measurement projects, for example, using advanced analytical techniques (such as correlation and data mining) to identify meaningful relationships within the growing body of measurement data
- Learning from metrics successes and failures, both our own and third parties, for example, drawing on employees' experience of security metrics used by other organizations
- Learning from metrics and measurement methods used in other fields, for example, health and safety, engineering, IT, medicine, quality, etc., and conversely, applying the lessons learned from information security metrics to those other fields and their measurement systems (see Section 5.3)
- Reviewing and updating the measurement requirements and the PRAGMATIC criteria in the light of experience
- Seeking independent advice on the measurement system and perhaps benchmarking it against similar organizations

Measurement systems have a natural tendency to grow continuously, gradually accumulating more and more metrics offering less and less value. Metrics that have

outlasted their utility become a costly bureaucratic burden on the organization, yet it is rare to find any systematic processes in place to identify and retire them.* This is an insidious problem for large, heavily regimented or regulated institutions and group structures with their long tenuous paths for management information. While it is relatively easy for anyone in power to justify and introduce additional metrics, it is much harder to identify, let alone retire, metrics that have reached the end of the road. An accumulating burden is the natural result.

A policy of one in, one out (each metric added to the measurement system must be accompanied by the removal of at least one other) may be the antidote. Alternatively, perhaps, a periodic cull of the worst-performing metrics. Either way, the PRAGMATIC method provides the means to distinguish high-scoring, high-value metrics in use from those low-scorers that offer marginal value and, hence, are prime candidates to be dropped. Done in this way, the retirement of metrics can be used to drive innovation, cut red tape, and save money—a nice triplet.

Yet another way is to follow the paper trail: trace the process from data gathering through analysis and report preparation through to its consumption and, most importantly, actual decisions and changes made as a result of the metrics. Obviously, any metric that never affects any decisions is not likely to be of much value.

Alternatively, if you're brave/foolhardy enough, you could just cut to the chase: quietly but judiciously suspend metrics that appear to be redundant and see (a) who notices, (b) who complains, and (c) whether they complain loudly enough to justify the metrics' reinstatement! This could even be deemed a metametric: the level of pushback when metrics are suspended is an indication of the extent to which they are being used and valued.[†]

As with retiring other information systems, you may possibly need to archive historical data from metrics that are being withdrawn, but if they are being permanently deleted as opposed to just suspended, this may be just another avoidable cost. The main caveat is that you may later need historical data to develop further metrics or test assumptions about cause–effect relationships. We can't solve that particular conundrum for you.

Last, take the opportunity to identify any lessons that might improve your ongoing metrics development efforts. Why did some metrics fail to justify their own existence? In what ways did the *information security measurement system* not fulfill its original promise? Which aspects were of the greatest value? If you were to do it all again, what would you do differently?

* It's the same crazy situation that leads us to carry on routinely filing the pink copy in box C even though nobody will ever read it, box C is quietly collecting dust on a shelf, and no one can lucidly explain what the pink copy was originally meant to achieve anyway.

[†] If you do take this approach, we suggest keeping the data collection and perhaps the analysis activities rolling for a while after you suspend delivery of the metric, just in case someone belatedly realizes the information was necessary for something after all.

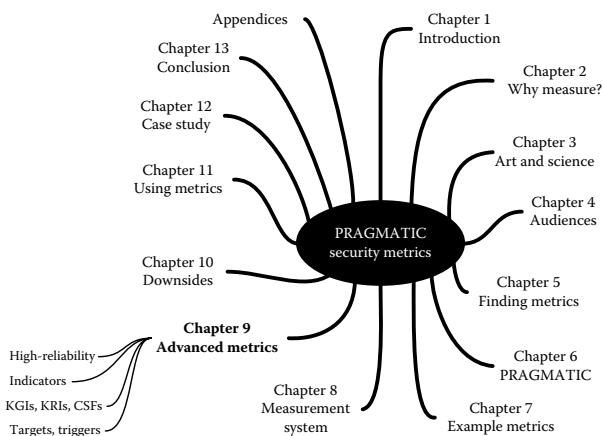
Tip: Even if you can't afford the resources to write up a full-blown eulogy to a dead metric, we suggest keeping a few rough notes in that little black notebook you routinely consult when contemplating changes to your *information security measurement system*. You've probably got it open right now, jotting down cool ideas gleaned from this book, no?

8.4 Summary

This chapter was about applying conventional systems and capability maturity concepts to the development of an *information security measurement system*, a coherent suite of valuable and mutually supportive metrics, rather than a more or less random assortment of individual security metrics.

Chapter 9

Advanced Information Security Metrics



We are saddled with a culture that hasn't advanced as far as science.

Michelangelo Antonioni

We don't mean to imply that the metrics practices we have discussed previously are retarded as such, rather that there are even more sophisticated considerations than we have so far considered. Many of the metrics issues discussed below have their roots in well-established disciplines, such as commerce/business management, science, and engineering. Compared to information security, or more accurately, IT

security,* they are highly mature, tracing their histories back literally thousands of years rather than mere decades. As information security professionals with an interest in metrics, we have a lot to learn from our learned colleagues in other disciplines.

9.1 High-Reliability Metrics

Metrics, like other processes, tools, and controls, sometimes fail. Unreliable instruments or measurement processes are annoying at best, misleading us with inaccurate, imprecise, or sporadic readings, implying that something is under control when, in fact, it is not or failing to alert us to conditions that require our attention. At worst, they can be a liability, occasionally creating grave risks and catastrophic consequences.[†] Consequently, every metric of any importance[‡] should be considered in terms of whether, when, and how it might fail and ideally engineered to make failure either extremely unlikely or conspicuously obvious. This section concerns the application of fail-safe and related reliability engineering concepts to information security metrics.

Safety-critical systems are the classic example. Many machines must operate within certain ranges for safety reasons: operating parameters exceeding acceptable limits would constitute a safety hazard, jeopardizing life and limb. The associated measurements are not only used to operate/manage the machines but also to confirm that they remain within safe limits, and hence, just like the machines themselves, the measurements must be more than just ordinarily reliable. Ideally, safety-critical machines *and* the associated measures and processes should fail safe, for example, if a nuclear reactor core temperature exceeds a limit value (indicating a control failure) or if the temperature readings don't make sense or stop altogether for some reason (indicating a measurement failure), the control rods are dropped automatically into the core to dampen the reaction. Approaches like these have developed over many decades of industrial design, applied engineering, and trial and error, learning from accidents, incidents, and near misses, and the learning process continues every day. We are presently behind the curve in information security.

Broadly similar principles can be applied to the design of business-critical processes, systems, controls, and measurements. High-reliability metrics are—or rather should be—an integral part of that mix.

A few information security controls arguably fall into the safety-critical category where the consequences of security failures are extreme hazards that threaten

* The Caesar cypher, for instance, is about 2000 years old. Hail Caesar!

[†] Speaking as someone who once ran out of fuel on an isolated stretch of road in the depths of winter because of the car's fuel gauge icing up and sticking at part-full when the tank was, in fact, empty, I have a healthy respect for the reliability of measurements and instruments.

[‡] ...and metrics of no importance are about as much use as ashtrays on motorbikes.

the health and safety of workers or the general public: generally speaking, such controls are protecting safety-critical IT systems. Many more information security controls could be deemed business-critical: their failure creates extreme risk and threatens the organization's survival. Consider the risks arising from, say, a complete failure of the organization's information access controls or the impacts of a disastrous loss of archived data resulting from a breach of the archive's security. Either way, it is sound engineering practice and could be considered prudent from a governance perspective to design the IT systems, processes, controls, and metrics, as a whole, to fail safe.

So how do we determine that our instruments might be misbehaving? What are the warning signs? Better still, what can we do to make critical metrics highly reliable?

The first step, because it is neither practical nor necessary to make *all* metrics highly reliable, is to identify the critical metrics through a process of risk analysis, focusing attention on them and determining the reliability requirements.* Because risk is the fundamental basis for information security, we won't belabor the point.

Next, apply sound engineering principles[†] to make the critical metrics highly reliable,[‡] such as

- Making the individual metrics and the associated measurement and reporting processes as robust as possible, essentially avoiding shoddy instrumentation and not cutting corners on quality
- Using self-tests or heartbeats to confirm the metrics are operating correctly (more below)
- Using duplication or, better still, triplication or *N*-plication[§] (multiply redundant measurements, instruments, measurement processes, and metrics, ideally avoiding single points of failure[¶]) with validation (cross-checking) to identify anomalous situations, making critical metrics more resilient to individual failures
- Preparing fallback/recovery arrangements just in case the critical metrics fail (e.g., send someone to observe critical activities directly, return to more fundamental metrics, or try to establish and fix the cause of the metrics failures)

* The engineering design risk management technique failure modes and effects analysis (FMEA), for instance, takes into account not just the probability (called "occurrence") and impact ("severity") but also the likelihood that failures will be identified ("detected") prior to a disastrous incident occurring. Food for thought?

[†] You probably recognize these as business continuity controls; the principles are the same.

[‡] There is an argument for making *reliability* one of the PRAGMATIC criteria for safety- or business-critical metrics. Feel free to adapt the PRAGMATIC approach accordingly if this is appropriate to your situation.

[§] Normally, we would adopt the fewest metrics necessary to provide all the essential information, avoiding superfluous metrics that simply increase costs and distractions.

[¶] Also known as *common mode* failures.

- As a last resort, preparing generalized contingency arrangements to deal as effectively as possible with whatever metrics crisis occurs*

The cockpit instruments in commercial aircraft and the operating/management consoles for complex manufacturing processes, such as oil refining or power generation, typically achieve high reliability using instrumentation that is both solidly engineered and cross-referential.[†] Critical systems, subsystems, processes, functions or parameters are measured by separate instruments. Any disconnect or failure is readily observable and can then be assessed.[‡]

Part of the fail-safe approach is a self-test or heartbeat function for the instruments and measurement systems. Even the relatively simple electrical/electronic dashboards of modern automobiles have a self-test mode when the ignition is switched on, checking and confirming the systems—particularly safety-critical elements, such as braking and air bags—and instruments are working as expected. Drivers are instructed to act appropriately if the warning lights don't extinguish after the vehicle starts up.[§] Instrument self-testing can involve injecting the kind of data that are supposed to register full scale on the meters or trigger an alarm condition (perhaps by momentarily simulating a situation such as conflicting indications that are supposed to generate warnings). The heartbeat approach involves the instrument expecting a certain number of data points every period: if the data flow stops (e.g., if the measuring device or data connection fails), the instrument raises the alarm in some manner. Intelligent measurement systems sometimes generate and monitor steady streams of specially tagged test data for this purpose.

While we can measure the same thing multiple times (i.e., multiple readings on the same or separate instruments), using different measurement methods or measuring separate but related parameters (e.g., different parts of the same business process) further improves reliability. In the information security context, a common example involves using antivirus software from different vendors to check mail servers and desktops and monitoring at the firewalls for anomalous network

* In information security, how *would* we fly blind? What does flying blind even mean in your context?

[†] In an aircraft, the artificial horizon shows the aircraft's attitude, the turn and bank indicator shows if the wings are level, the compass shows if the aircraft is turning, and the altimeter and airspeed indicator show if the aircraft is descending (speed increasing) or ascending (speed decreasing). By systematically cross-checking between these readings, any inconsistencies alert the pilot to an anomaly, perhaps a problem such as an instrument failure. For example, if the artificial horizon shows the aircraft pointing down, and the rate of climb indicator says it is descending, but the altimeter shows no change in altitude, something strange is going on: most likely the aircraft is in an updraft, but possibly the altimeter is malfunctioning.

[‡] The reliability-engineering approach applies to the design of critical security controls as well as critical metrics. If the firewall rules are supposed to block certain types of network traffic, but a network sniffer detects that sort of traffic, evidently something is amiss.

[§] Unfortunately, few notice the tests. Do you recall whether *your* car does this? Does it do an “all lights lit” test too?

Tip: There is a natural human tendency to place undue reliance on automated systems, including their fancy, real-time graphic displays and management consoles, but when they fail unexpectedly after years of consistent operation, the results can be catastrophic.* Aside from making the metrics and measuring instruments more reliable, don't forget that *humans are a vital part of the system.*†

* The ability to identify and respond to anomalous measurements and failing instruments instantly is one of many enormous advantages to SCADA. At the same time, failure of the SCADA system itself could be disastrous for the operators of a factory, power station, or aircraft, so there are good reasons why totally independent (often good, ol' fashioned electromechanical) instruments are also used to monitor the most safety- or business-critical parts of the plant.

† Understanding the possible reasons for conflicting instrument readings and knowing what to do about them is a key part of pilot/operator training. Maybe you should include metrics in your security awareness/training program.

connections or traffic. Mundane metrics (such as the number of viruses, Trojans, etc., detected per day) pale into insignificance compared to, for example, an alert from the network administrators that one of the corporate servers is streaming 1GB of encrypted traffic per minute to an unknown server in China!

9.2 Indicators and Proxies

Many of the information security-related things that we would like to quantify are difficult/expensive and sometimes literally impossible to measure directly. Perhaps the most glaringly obvious example is information security risk itself: uncertainty is an inherent, integral, and inalienable property of risk, the very essence of risk, in fact, because once a risk materializes and an incident happens, it has become a certainty and is, strictly speaking, no longer a risk.*

In such situations, we may have little option but to use proxies, artifacts that stand in for whatever it is that we are concerned about without directly measuring it.

A common approach to quantifying information security risks involves measuring, or at least assessing the general scale of, the component parts of risk, namely, the threats, vulnerabilities, exposures, and impacts. For example, the number of viable threats we can identify through analysis would be of interest when assessing the risk associated with an application system as would the number of exploitable technical vulnerabilities we know about (and perhaps an estimate of the number that are most likely in there but not yet recognized as such), an assessment

* OK, if you *insist*, it is a risk with a probability of occurrence of precisely 1. Get a life!

of the extent to which the system is exposed to the threats of most concern, and the importance or criticality of the system to the business (which is a proxy for the impact component).*

In much the same vein, indicators are telltales, meaning observable characteristics or features that are associated with, rather than part of, the thing of interest. In relation to information security risk, again, one indicator is the number and gravity/severity of incidents and near misses that have happened. Absent other clear warning signs, a marked increase in the number of reported industrial espionage incidents strongly indicates an increase in the risk of industrial espionage. The link is not absolute,[†] but it takes a brave (or foolhardy!) manager to argue the converse and ignore the obvious warning signs.

Corporate security culture is another example. It is technically possible to measure corporate security culture in a scientific manner using psychological/anthropological research methods, but it is generally impracticable to do so (not least because of the difficulty of defining it precisely enough to study). Proxies include various, more readily observed, behaviors, such as the extent of employee compliance with policies, etc. and employee attitudes toward security as revealed by surveys. It is pretty obvious that a resentful, demoralized, indifferent staff is less likely to take a personal interest in carefully managing risk and compliance rules than one that is not. Absenteeism, rising levels of infractions, the general nature and tone of emails (a field of study called sentiment analysis), collective torpor, water-cooler mutterings, or the more contemporary version, griping on social media, are all potential indicators of the corporate security culture.

Indicators and proxies are useful because they correlate, to varying extents, with information security aspects of interest. We have more to say on correlation and other statistical methods in Chapter 11.

9.3 Key Indicators

9.3.1 Key Goal Indicators (KGIs)

We introduced the capability maturity model (CMM; Paulk et al. 1995) in Section 3.8 as one of several ways to define metrics requirements and described the definition of information security goals supporting business outcomes. KGIs are metrics that relate to those goals.

For most organizations with critical or sensitive information assets, particularly highly regulated organizations in the financial services and telecoms sectors, CMM level 4 represents an adequate level of protection, though one not easy to attain. The

* While still relatively crude, we much prefer approaches of this nature over more theoretical objective risk analysis methods that appear to us somewhat divorced from reality, given the distinct lack of factual data for their projections.

† Perhaps the number of incidents is the same as ever, but more are being reported.

version of CMM in the CISM Review Manual (ISACA 2012) states the following 15 requirements to achieve level 4:*

1. The assessment of risk is a standard procedure, and exceptions to following the procedure would be noticed by information security management.
2. Information security risk management is a defined management function with senior-level responsibility.
3. Senior management and information security management have determined the levels of risk that the organization will tolerate and have standard measures for risk/return ratios.
4. Responsibilities for information security are clearly assigned, managed, and enforced.
5. Information security risk and impact analysis is consistently performed.
6. Security policies and practices are completed with specific security baselines.
7. Security awareness briefings are mandatory.
8. User identification, authentication, and authorization are standardized.
9. Certification of security staff is established.
10. Intrusion testing is a standard and formalized process leading to improvements.
11. Cost–benefit analyses, supporting the implementation of security measures, are increasingly being utilized.
12. Information security processes are coordinated with the overall organization security function.
13. Information security reporting is linked to business objectives.
14. Responsibilities and standards for continuous service are enforced.
15. System redundancy practices, including use of high-availability components, are consistently deployed.

Each of the 15 statements can provide the basis for a KGI and, for that matter, one or more policy statements. KGIs may also need to be developed for intermediate steps of multiyear projects that might coincide with budget cycles, for example.

9.3.2 Key Performance Indicators (KPIs)

KPIs are the measurable steps along the way to achieving a KGI, used to track progress. The same CMM level used to set objectives can also serve as a KPI to determine maturity progress toward the objective. Other performance indicators may be used to track budgets and project completion steps. KPIs are used to populate a project roadmap, and their sequence should be subject to critical path analysis to ensure various project steps don't interfere with each other, for example, if one step

* ISACA's straightforward narrative is comprehensible even by business types. In case the advantage isn't blindingly obvious, try explaining a balanced business scorecard or a computational model, such as VAR, to the uninitiated!

in the roadmap requires the installation of a database, obviously the supporting infrastructure must be provided first. Conflicting resource requirements will also be highlighted by this process.

9.3.3 Key Risk Indicators (KRIs)

Careful post hoc analysis of serious information security incidents almost always shows a series of precursor events and changes that could or should have raised the red flag on the associated risks that eventually materialized. Some risk factors are glaringly obvious in hindsight, such as a dramatic rise in incidents in your industry sector or location (increasing threat), a stack of security patches waiting patiently on the side for their chance to be implemented (increasing vulnerability), or changes that led to business processes becoming critically reliant on certain information sources or systems (increasing impacts). Other risk factors may not be so clear, but it is unusual for major incidents to happen totally out of the blue.

Aside from investigating the causative factors in order to resolve them, post-incident reviews should also explore the question of why the warning signs (i.e., the KRIs) were missed at the time. What were the KRIs, and how come they either weren't being monitored or failed to trigger appropriate responses that would have prevented or lessened the incident?*

Many information security metrics could be classed as risk indicators: the difference with KRIs is simply a matter of degree; "key" implying "important" or "critical" or "miss this and we're sunk." KRIs are therefore highly context-dependent, so the example KRIs below may not be applicable in your organization:

- Unusual numbers of change requests, especially emergency changes
- Substantial increases in employee turnover or absenteeism
- Substantial increases in policy infractions, noncompliance/exceptions, and exemption requests

Tip: Seize the day! Incidents often highlight concerns over the risk analysis and risk monitoring/tracking processes that evidently missed the threats, vulnerabilities, exposures, and impacts. In the aftermath of an incident, managers may argue over the details and dispute accountability, but that there actually *was* a risk is an indisputable, unavoidable, iron-clad fact, whereas it appears not to have been noticed or addressed adequately beforehand.

* If it appears that an incident was caused not by the lack of warning about the risk but by the failure of one or more security controls, that simply moves the focus of attention to the suitability and effectiveness of the controls, indicating unmanaged risks in that specific area.

Tip: Despite the obvious advantages, organizations with immature approaches to information security seem curiously reluctant to undertake post-incident reviews. We suspect the ability to identify and, especially, to learn from one's mistakes correlates strongly with an organization's overall information security capability. Whether or not you agree with us, take a long cold look at Figure 7.2 and ponder the incident management metrics examples in Section 7.10. Are you doing enough to capture the lessons? Are your KRIs being actively tracked?

- Delays/inconsistencies in patching
- A series of highly critical audit reports

KRIs are about identifying and doing something to avert those accidents waiting to happen. Often the solution lies in an escalation path to senior management for security issues that have been building for some while. Strategic-level Predictive and Relevant metrics are therefore likely to qualify as KRIs.

9.3.4 Critical Success Factors (CSFs)

They may not have “key” in the name, but CSFs are conceptually related to KRIs, KPIs, and KGIs. CSFs are things deemed essential to achieve some goal, objective, or outcome. Businesses, business units, departments/functions, projects, and activities can all have CSFs. Because they are critical, CSFs are self-evidently prime candidates for measurement.

Information security CSFs obviously relate to information security department/function, projects, and activities (particularly the information security goals shown in Figure 3.2) but also occur in related fields (such as risk, compliance, and audit) and in unrelated fields and business activities whenever they identify a critical reliance on either information or information security (e.g., in relationships with third parties providing, processing, storing, and transporting vital information).

9.4 Targets, Hurdles, Yardsticks, Goals, Objectives, Benchmarks, and Triggers

As soon as something is measured, we have the possibility of comparing it rationally against comparators, such as

- Previous measurements of the same metric (giving us historical trends and self-improvement)

- Projected or predicted measurements (giving assurance as to our predictive capability)
- Variously defined ideal values (see below)
- Other similar or related metrics (allowing us to cross-check or validate particularly important metrics)

Common factors are (1) having reference points against which to assess/compare the measurements and (2) the presumption, urge, desire, or demand for the subject of measurement to meet or exceed expectations.

The reference points and ideal values include the following:

- *Targets*, for example, reducing spam messages reaching employees' inboxes below 1% of emails received
- *Hurdles*, for example, getting 80% of the security policies formally approved by management this year
- *Yardsticks*, for example, reaching CMM level 3 for our information security practices
- *Goals and objectives*, for example, supporting the safe, controlled introduction of an online sales platform
- *Benchmarks*, for example, being rated by a broad-based information security survey in the top quartile of organizations in our industry for all categories of concern
- *Triggers*, for example, if the rate of password resets exceeds 10% of help desk calls, review and repeat the associated security awareness activities

Notice that the comparisons, and thus the metrics, do not necessarily have to be strictly numeric:^{*} being certified compliant with ISO/IEC 27001 is a good example of a meaningful metric, a standard of achievement that is not itself a matter of earning so many points from the certification assessors. There is no simple pass mark for certification. It comes down to an accredited certification body's informed opinion on whether the organization satisfies the mandatory requirements for an information security management system that are explicitly stated in the standard, *plus* provides sufficient, credible evidence to prove the system both meets the organization's information security objectives (as specified by management in the statement of applicability) and is operating correctly.[†]

* We beg to differ with those who insist that metrics generate numeric or number-and-unit outputs (e.g., 27 incidents or \$3 million). Disregarding measurements that do not generate numbers is a retrograde step, in our opinion. But what do *you* think?

† Admittedly, satisfying or failing to satisfy the standard's mandatory requirements is a binary measure, but the other aspects are certainly analog. In practice, numbers really don't come into the equation: certification is a question of judgment, not mathematics.

Critical metrics that have to be interpreted and acted upon by humans, especially those with defined key values (the minima, maxima, or trigger levels), are often supported by warnings, alerts, and alarms. The terms imply a natural priority sequence:

- The first-stage indication of possible trouble is a low-grade warning of some kind, such as an email or warning message on the console, meaning “This does’nae look good, Jim.” Warnings are released some distance from some key value,* the distance being a configurable parameter.
- The next stage, indicating there is definitely a problem needing to be addressed, raises some sort of alert—perhaps sending a pager message or flashing a console message in bright red and sounding a buzzer to mean “She can’nae take much more of this, cap’n!” Alerts are also released at some lesser, configurable distance from the key value.
- If the metric continues to worsen and hits the key value, the ultimate stage is an alarm that is even harder to ignore—perhaps a klaxon or bell meaning “BRACE YOURSELVES FOR IMPACT!!”—or an automatic response to bring the system to a known safe state (normally an emergency, but still controlled, shutdown).†

The configuration of suitable levels is clearly crucial to the sequence. Configuring and (where appropriate) adjusting the levels is an integral part of designing and implementing the metrics.‡

9.5 Summary

This chapter explored still more advanced aspects of security metrics, dealing with issues, such as making critical metrics more resilient, measuring risks, goals, and performance (KGIs, KRIs, KPIs, and CSFs), and using metrics to set targets.

* The key level is usually determined by a professional risk-based assessment, perhaps bearing some relationship to a defined value, such as a compliance requirement or a physical value, such as the melting point of dilithium crystals.

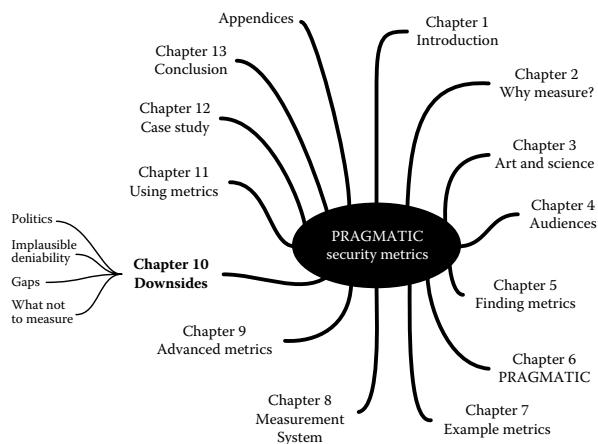
† It is possible to link security metrics into the incident management process, for example, a security metric going into the red is itself treated as a security incident, triggering the conventional incident analysis, identification and allocation of resolving agencies, damage limitation, corrective actions, and post-incident review activities. Be sensible about it if you take this approach, however, because not all adverse measurements deserve the full treatment, and you risk burying significant issues under trivia. Limit it to the KRIs, for example.

‡ Sophisticated, modern SCADA systems overseeing computerized plants are able to adjust some of the levels and the nature of the warnings generated dynamically according to the unfolding situation because a serious incident may generate so many alarming conditions that the hapless operators are at a loss as to what to do first. Prioritization is the name of the game with obvious application to information security. The PRAGMATIC scores are a way to prioritize the presentation of metrics statically or, rather, to propose a prioritization, allowing management to make the final determination. You are on your own when it comes to the dynamic aspects, however.

Free ebooks ==> www.ebook777.com

Chapter 10

Downsides of Metrics



But everything you do in life has a downside.

Melissa Auf der Maur

This chapter acknowledges that although there are tremendous advantages to selecting and using appropriate information security metrics, there are also a few drawbacks.

10.1 Numbers Don't Always Tell the Whole Story

Be careful what you wish for! A suite of PRAGMATIC security metrics, particularly within an *information security measurement system*, will provide the information management needs to manage information security to a large extent scientifically

(by the numbers). However, information security is a branch of risk management. Even with the world's greatest *information security measurement system* comprising a suite of the most PRAGMATIC security metrics, we must not ignore the fundamental fact that we are dealing with things that are, to varying extents, inherently unpredictable.

We might be able to tame information security risk, but we will never domesticate it.

As a consequence, there are inherent unpredictabilities with some information security metrics. We can do our level best to minimize them by using better, more reliable instrumentation and to smooth them out using the statistical techniques described in the next chapter, but they inevitably remain.

Sometimes someone with sufficient experience in the area—you, perhaps—may feel the numbers simply don't add up: the metrics indicate a particular course of action that, for some reason, your experience tells you is not appropriate. Such discrepancies may be distinctly unsettling at the time but can be fascinating to examine in more detail:

- Is it that the numbers truly are lying, perhaps because the raw data are wrong or the analysis is faulty?
- Are the numbers misleading because they don't take sufficient account of all the relevant factors (meaning the model or framework underpinning the metrics is flawed)?
- Has something changed, so the metrics no longer make sense?
- Or is that the numbers and analysis are, in fact, correct, but for once, your gut feeling has let you down?*

If the *information security measurement system* is generally sound enough to have proven itself trustworthy, the latter conclusion may be management's default presumption in the absence of compelling evidence that something else is to blame. In other words, management may need to be convinced not to do whatever the metrics are suggesting but to follow a different course.[†]

The issue of trusting your metrics is superbly demonstrated by experiments performed by the U.S. Navy way back in the 1940s brought about by an increasing number of aircraft accidents in zero-visibility conditions, such as flying into clouds or heavy fog. It turned out that even the best pilots were unable to fly straight and level for less than half a minute using just their senses. This led to the development of instrumentation that is used today for flight under those conditions, known as IFR or instrument flight rules. Acquiring an instrument ticket is typically the most arduous licensing, and the requisite is absolute trust in the instruments—properly

* Such is the route to enlightenment, Grasshopper.

[†] This is a distinctly dangerous route to take, especially if the measurement system is mature, as it devalues and may even discredit the measurement system in the eyes of the more cynical and thoughtful managers anyway.

Tip: Naturally, it is best not to land in this situation! It helps if the more complex information security metrics are routinely interpreted for management, not in the sense of being selective or economical with the truth, but providing the context and framing the analysis in such a way that information security management—including the use of security metrics—is plainly an uncertain risk-based activity.

cross-referenced to spot anomalies or instrument failure—even when the senses indicate the contrary. There may be a lesson here for the astute security manager.

The subtitle to Andrew Jaquith's book *Security Metrics: Replacing Fear, Uncertainty, and Doubt* (2007) hints at a related issue. It is all too easy for information security professionals, who are naturally risk-averse, to overemphasize information security risks, especially where, regardless of the availability of relevant metrics, the basis for projecting and assessing the likely magnitude and probability of risks is dubious or shaky.* There are plenty of opportunities in interpreting the results of benchmarks, security surveys, and other reports for management to pick up and raise security issues, and metrics, either out of context or inappropriately.

10.2 Scoring Political Points through Metrics

A particular concern in some organizations or situations is the selective use or portrayal of specific metrics to support a biased argument, deliberately ignoring or downplaying those that counter or detract from it.[†] To an extent, we all do it—it's called making your case and justifying your existence or selective memory or biased

Tip: As information security *professionals*, we have ethical responsibilities toward the profession, our employers, and ourselves. That includes using metrics honestly, ethically, and responsibly. Scaring management into investing in security is itself a risky strategy because it might call your bluff and accept the risks (perhaps unwisely) or accept your argument but later discover the controls you proposed are not completely effective—either way, your personal credibility may be irreparably damaged.

* See Appendix J.

[†] The biases detailed in Appendix J apply to *us*, not just other people. We do, at least, have the advantage of self-awareness and can perhaps make use of the techniques described in Appendix K to counteract our biases.

Tip: If this is a serious possibility, you may prefer to forestall it by discussing the possibility with senior managers when the *information security measurement system* is initially designed and implemented and when it is periodically reviewed and improved. At least then you will be understood when you delicately point out that the security metrics were never intended to be used to further personal agendas.

assimilation. In some politically charged organizations, there is also a real danger that certain managers may deliberately interpret the security metrics reported or available to them in a highly selective or misleading way to further their own personal goals and private agendas. Be prepared for them to dig deeper into, if not openly misuse, the raw data to find hard evidence that you didn't anticipate—for example, explicitly comparing the cumulative cost of security incidents between departments in order to point out that *their* department is angelic while department X is horribly insecure.

10.3 Implausible Deniability

Information concerning governance, risk, security, control, and privacy issues within the organization—including information security metrics—may become a hot potato if management is accused of failing in its associated compliance responsibilities following a security review, audit, or, worst of all, a significant incident. It cannot plausibly deny that it knew about the issues if there is evidence to the contrary, such as management reports containing metrics indicating a serious problem with security. If such accusations are raised in the media or, worse, in court, there is nowhere left to hide.

This is another good reason for being cautious about which security metrics are reported to senior management. Not only are managers invariably busy dealing with lots of issues competing for their attention, but they may be personally accountable for failing to identify and act on serious matters that have been brought to their attention—and, in fact, that phrase hints at a further concern. The way metrics are reported, in particular, the manner in which significant issues are or are not highlighted, presented, and discussed, is relevant here. We're talking about the distinctions between data, information, and knowledge:

- *Data* are the raw numbers, indicators, statistics, and other details that have little inherent meaning or value without analysis.
- *Information* is the valuable meaning that emerges from rational analysis and consideration of the data. This is where highlighting significant values comes

Tip: Managers may be unwilling even to discuss issues of this nature openly as doing so acknowledges that they are aware of the possibility. It's a sensitive area, so tread lightly if you do decide to raise it. Off-the-record conversations may be the best you can achieve. Be very wary of putting anything in writing unless you already know for certain that you have senior management support.

into play—to quote Peter Drucker, information is “data with relevance and purpose.”

- *Knowledge* is the understanding, the golden nuggets or pearls of wisdom among the available information that facilitate and lead to appropriate decisions being made on the basis of that information—in other words, actionable information.

It may seem a reasonable defense for the CEO to claim, for instance, that he or she didn't appreciate the gravity of the vulnerabilities in the database access controls that led to a serious privacy breach because that mere technical detail was buried in the depths of an unfathomable management report. From a governance perspective, however, the CEO is accountable for the nature of the reporting and thus the measurement system as well as the decisions arising from it.

10.4 Metrics Gaps

Some aspects of information security may not be being measured in a PRAGMATIC way right now for various practical reasons in your organization, potentially leaving coverage gaps or holes in your *information security measurement system*. The lack of metrics in some areas carries the risk that those aspects may be ignored or down-played by management in favor of addressing others where the numbers indicate significant issues or improvement opportunities.

The ideal way to resolve this issue is to identify and work on closing the gaps, of course, and extending the coverage is an important element of maturing the measurement system alongside improving existing measurement processes and metrics. Meanwhile, it helps, at least, to identify and acknowledge the gaps.

It's easy to get carried away with metrics, introducing more and more of them until you end up with a panoply of individually justifiable measures that overwhelms the audience. The costs of running a large measurement system obviously detract from its financial value while its complexity creates more subtle organizational problems, such as the feeling of perhaps being deliberately misled by the numbers (wool-over-the-eyes syndrome).

Tip: We wrote about the issue of how many metrics to short list earlier—it's an important issue in the design phase in Section 8.3. Taking care of this at this early stage (perhaps even earlier, e.g., during the specification or architecture and design phases) helps avoid it becoming a problem for you later on. Otherwise, you may have little option but to resort to metrics culls and similar drastic responses to rescue a failing *information security management system* from collapsing under its own weight.

The approach to determining whether you have too many metrics is pretty straightforward: if it's information nobody needs or wants, continuing to provide it would be counterproductive. On the other hand, if there is information someone has identified as useful or necessary, by all means develop a process to supply it if feasible from both a cost and process perspective.

10.5 On Being Good Enough

There is a natural tendency when developing and using metrics to overemphasize the accuracy, precision, and validity of the measurements in a strictly scientific or mathematical sense. This aspect shines strongly in some of the other books on this topic, which *insist* that metrics must be both *numeric* and *objective*, thereby discounting potential metrics that are being used and are patently useful, despite being narrative and subjective. Some of the arguments are perfectly valid (e.g., conventional arithmetic is meaningless for ordinal values and, in fact, can be distinctly misleading just as there are lies, damn lies, and statistics), but this line of reasoning can be taken too far. It implies that management is a precise, scientific discipline. Hello?

There may be no objective, scientifically proven, generally accepted, numeric measure for security status, but management may be very concerned to discover that our security status has declined to an all-time low. Those evocative words are indicative of the underlying situation, which may or may not have been measured by a raft of objective, scientific metrics. The true purpose of such a statement, albeit subjective and perhaps even inflammatory in style, is generally to bring matters to a head and prompt management to *do something positive about it*. All scientific or mathematical niceties aside, the information security manager's or risk manager's gut feeling based on years of professional experience may give such a statement the credibility it needs even without all the numbers to prove it.

Striving for perfection in security metrics can be counterproductive when good enough will do. For example, it is technically possible to undertake a scientific study or survey of employees to measure their perceptions about the readability of

the organization's information security policies and procedures. One could call in a consultancy to run such a check and set a baseline, make changes to the policies and procedures, and then remeasure to determine how much things have improved. Studies of this nature are not free, however. Aside from the time and resources needed to specify, develop, conduct, analyze, and report, the participants generally also have to put some time and effort into responding to surveys and perhaps poring over the detailed appendices in the management reports. Furthermore, after investing so much in such a project, it is inconceivable that the metrics would ever be used to demonstrate a *reduction* in the readability—in other words, the result is a foregone conclusion. Meanwhile, management may have been perfectly willing to accept that the policies and procedures need updating and happy to assign the resources to do it rather than measure it.

In this respect, we don't entirely agree that you can't manage what you can't measure... *if* it is taken to imply...scientifically. Gut feeling and experience have always been part of management, and we don't anticipate that situation changing much in our lifetimes. Subjective impressions and opinions really do matter in the real world, especially in the case of high-status individuals who wield corporate power. Perhaps the best we can hope for is to influence management decisions concerning information security through more poignant, credible, and convincing metrics—and that, to us, is a very worthwhile objective, so please don't knock it just for the sake of science and mathematics.

Management's trust in your security metrics is arguably something you must earn rather than demand. The metrics must earn their keep by proving themselves reliable, credible, and, most of all, valuable. If this is of concern, you can help matters by using metameetrics to establish their reliability, credibility, and value. Also, but more prosaically, you can simply point out "I told you so" when predictions come true—but tread lightly as this can be a very unpopular message and one that may be thrown back in your face when things don't go according to plan!

10.6 What Not to Measure

We thought it would be interesting, fun even, to point the finger at a few of the security things that are commonly measured and reported, despite having little value to management:

- *Spams received:* we have negligible influence over the number of inbound spams, so while the numbers may be vaguely interesting in a hand-waving, "Golly gosh" sense, they are not of much practical use. Spams that got past the anti-spam filters (false negatives) might be a better metric as at least we have some control over that, but combine it with legitimate emails incorrectly blocked as spam (false positives), and we're really starting to get somewhere.

- *Viruses blocked:* trust us, nobody outside of information security honestly cares how much malware was blocked. “How many viruses got through?” they ask. We can only give a partial answer because we can only count the ones we detect—and the remainder (if any) is really scary.
- *Technical security vulnerabilities resolved:* this is old news, of course, and tells us nothing about how many technical or, indeed, nontechnical security vulnerabilities still remain. At a push, the metric might be a rough guide to the amount of effort being expended on patching and updating systems, but if that is genuinely of concern to management, there are surely better measures.
- *Compliance* sounds, at face value, like something management might want to measure, but don’t lose sight of the true goal—to obtain the benefits of compliance rather than compliance per se. If we focus too heavily on compliance, we risk divorcing the strict, literal wording of the requirements from their honest meaning and intent and driving strict, literal compliance, whereas bending—and on rare occasions consciously breaking—the rules might, in fact, be the best option for the organization. Measures of compliance may be a worthwhile spinoff from the *information security measurement system*, but compliance itself should not be the sole driver.
- *Metrics that are easy and cheap to obtain*, simply because of that fact, despite their being unrelated or only marginally linked to identified security objectives: these metrics just add noise, distracting management from the *stuff that truly matters*. Cost is merely one of the PRAGMATIC criteria, and even that is best understood as value.
- *Metrics with PRAGMATIC scores significantly below those of any other metrics that you are not currently using:* by consistently and systematically selecting high-scoring metrics while, at the same time, preferably retiring current metrics that score badly, you are incrementally raising the overall quality of your *information security measurement system*.
- *Metrics that we or anyone else recommends*, purely because they are recommended: your requirements are unique. We barely have a clue about the kinds of security things that might be important to your organization or the nature of the security risks and issues you are grappling with. Think of this book like generic healthy living advice on the Web, as opposed to a consultation, diagnosis, and prescription from a qualified doctor. To put that more succinctly, YMMV.*

* YMMV usually means “your mileage may vary,” a classic example of a product disclaimer, used to explain why the headline fuel consumption figures on the glossy advertisements for new cars turn out to be unachievable in practice. Here, we mean “your metrics may vary,” but the rationale is much the same.

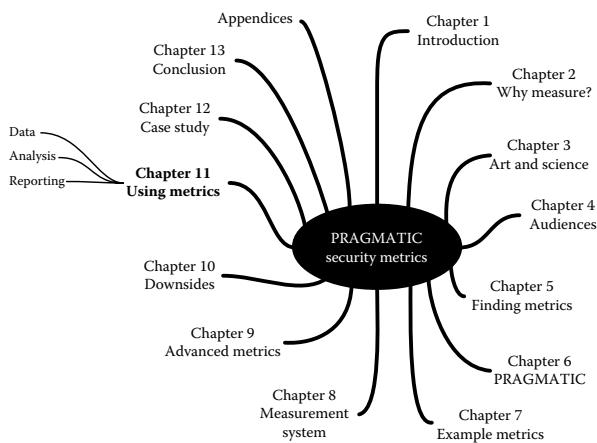
10.7 Summary

This chapter was a short disposition about the drawbacks of information security metrics, including the ways that security metrics may mislead or be misused for political purposes and personal agendas, plus some things that are unlikely to be worth measuring, ever.

Free ebooks ==> www.ebook777.com

Chapter 11

Using PRAGMATIC Metrics in Practice



Dream in a PRAGMATIC way.

With apologies to Aldous Huxley

Aside from the issue of which metrics you select, the way in which metrics are *used* can make a huge difference to the effectiveness of your *information security measurement system*. Because it would be a terrible shame to see all your hard work go to waste, this chapter offers guidance on how to position and use metrics more effectively.

Before we continue, there's something we need to just mention. We are practitioners and pragmatists by nature, not statisticians or academics. This book is firmly grounded in the *real world*. If you have come to this chapter for advice on chi-squared tests or Poisson distributions, you will be sadly disappointed. We profess only basic and limited knowledge of statistics and number theory—enough to get by. For the more complicated stuff, we rely on our old friend Mr. Google and, on rare occasions, the dog-eared statistics textbooks from our college studies many moons ago.*

11.1 Gathering Raw Data

Metrics, of course, depend on measurements[†] and analysis of the raw data—the numbers that underpin them. There are many different sources and ways to gather raw data, and we don't intend to go into great detail here, apart from mentioning a few techniques that we have found useful in practice.

11.1.1 Sampling

In situations where it is infeasible, inappropriate, or impossible to measure every single member of a population,[‡] measuring a sample instead will give statistically valid data for the entire population *provided* the sample is scientifically selected. The selection of samples should ideally be randomized and unbiased, meaning (1) samples should be selected in such a manner that every member of the population has an equal chance of being selected, and (2) the selection of new samples should not depend in some way on samples previously selected. The sample also has to be large enough to be considered statistically representative of the population from which it is drawn.[§]

Various sampling approaches are used routinely by auditors if they cannot reasonably check the entire population of interest. For instance, when checking the accuracy of the payroll, auditors may select a bunch of people at random from the payroll file and confirm that they were paid correctly. The number in "a bunch" often depends on their initial findings: if no errors are detected in the initial sample,

* Better yet, we find *someone who knows* and ask him or her to do it for us.

† Metrics also require one or more points of reference. Six inches is a measure but pretty meaningless without reference points. Six inches *from* something or *between* two specific points provides the context and relevance.

‡ 100% sampling is generally not cost-effective unless the population is small, for example, seeking the opinions of all executive managers.

§ The level of variability in the population is relevant: if the population is quite consistent (i.e., low deviation, all members tightly cluster around the mean value), fewer samples are needed. However, the reason we are measuring is generally that we don't know how variable the population is, hence the rule of thumb that follows.

Tip: As a rule of thumb, 30 is a practical minimum sample size for statistical validity unless the population being sampled is small. For example, aim to collect *at least* 30 responses from workforce surveys.

the auditors may move on to other, more promising lines of investigation, whereas if there are loads of errors, they may take and test a larger sample in order to gather statistically valid data (e.g., the mean error) and so substantiate their findings (e.g., we calculate approximately \$50,000 of overpayments per month). Furthermore, the sample may be selected not to achieve statistical validity necessarily but on some other basis, perhaps to test an audit hypothesis (e.g., rank last month's salary payments according to the difference in value from the previous month and select the top 50 records by difference value for testing).

In practice, many business decisions are made without the benefit of statistically valid data, although, arguably, having a more scientific basis would improve the quality of those decisions.* This *is*, after all, a book on metrics!

11.1.2 Automated Data Sources

Automating the collection, analysis, and reporting of information security metrics has obvious benefits:

- The tedious manual effort is reduced.
- Once established and operational, costs are reduced, freeing up staff/management time for other business activities.
- The data processing runs like clockwork, meaning regular reports are scheduled automatically to arrive on time, and (provided the automation is well designed and implemented) the results are generally as accurate and complete as they can be.

However, there are also drawbacks to automated metrics processing:

Tip: Speak nicely to your auditors for advice on sampling and statistics.

* Even statistically valid numbers may not be sufficient for security purposes. If every single one of a random sample of 10% of the organization's servers is properly patched, for instance, it is not unreasonable for management to infer that *all* the servers are properly patched. However, even a single unpatched server among thousands that are fully patched may create an unacceptable risk, while even fully patched servers remain vulnerable to zero-day exploits.

- The selection of data and metrics may be skewed by the ready availability of certain automated data rather than by management's demand for useful information. Consequently, worthwhile metrics drawing on data sources that cannot be readily automated may be neglected.
- "Attempting to automate measures that have not yet been thoroughly tested and proven to be effective can be ultimately counterproductive" (Barabanov 2011).
- The implementation costs can be substantial because automated data sources, interfaces, collection, analysis, and reporting mechanisms all need to be defined, developed, tested, and installed. There are also ongoing maintenance and management costs, for example, ensuring various process and system changes do not affect the availability and integrity of security metrics data.
- Automated data processing can go wrong, for example, generating misleading or nonsensical outputs if the raw data are missing, incomplete, late, or inaccurate or if there are design flaws and bugs in the systems. These are, of course, information security risks, meaning security controls are probably required in the measurement systems or the associated manual activities. Stuxnet is another example of what can happen to automated systems and raises the issue of possible sabotage.

To illustrate the complexities of automating security metrics, consider the near-universal need for financial metrics relating to the cumulative costs of actual information security incidents. Where can we get the raw numbers? Many organizations track security incidents through conventional problems and request management support and call-logging systems run by the help desk. When an incident is first identified, someone logs a call with the help desk to initiate the incident management process. As various resolving agencies are assigned and do their thing, their activities are tracked against the trouble tickets until, eventually, the incident is resolved. Is it feasible to incorporate an "incident cost" field in the help-desk problem management system and ask resolving agencies to identify costs associated with the incident, such as their own time and materials, plus estimates of costs suffered by the business users? If so, then you potentially have your source of raw data, making it simple to generate reports feeding into information security management's regular

Tip: In practice, it is definitely worthwhile looking to automated data processing but *only*, we suggest, for those information security metrics that the organization actually needs—in other words, *metrics automation should be demand-led, not supply-driven*. Trying to find ways of using the automated data that happen to be produced by, say, a firewall system is not the most sensible approach unless there is genuinely worthwhile management or operational information in the firewall numbers.

management reporting processes. However, the fact that the incident cost metric involves estimations constrains its accuracy (particularly because the business costs are often the most substantial part of the impact) and renders it open to challenge—so much so that, despite the effort and costs involved in the metric, we end up not much better off than if someone crudely assigned impact levels and left it at that.

11.1.3 Observations, Surveys, and Interviews

It would be a serious mistake to discount measurements that are not made with a physical instrument such as a ruler, weighing scales, or counter as being inherently unscientific. Measurement is a vital part of modern biological and medical science, for example, just as much as in, say, physics or chemistry, although the methods sometimes differ. Human behaviors, attitudes, perceptions, etc., are typically measured using techniques such as direct observation, surveys, and interviews: provided they are well designed and performed, these are reasonably objective, repeatable, accurate, and—yes—scientific forms of measurement, and as such, they are valuable for information security measurement and management.

The phrase “provided they are well designed and performed” is worth exploring in more detail. There is generally a choice of measurement methods and subsidiary choices within each method. For the sake of illustration, let’s assume we want to measure the efficiency of our security administration processes. We might simply assign someone to watch the admins going about their daily activities in order to gather general impressions and perhaps time their performance of specific tasks using a stopwatch. The observer might take notes about the sequence of steps they perform or videotape them (perhaps secretly) for more painstaking analysis. The period of observation might last anywhere from a few minutes to a week or more. We might get a student to do the observing or employ a trained behavioral scientist, perhaps more than one, or we might simply ask the admins to keep their own activity records... Clearly, there are markedly different costs involved in the different approaches (not just in terms of the expense of employing the observers but also in the effects on the admins being observed) as well as different benefits (e.g., the quantity and objectivity of the data varies). At the end of the day, it comes down to someone making a business decision and perhaps conducting a limited scope trial to see how well it works out in practice.

Tip: Depending on what you are trying to achieve and the size of your budget, there is no harm in exploring measurement techniques used in such diverse fields as psychology (e.g., psychometrics), market research, quality, auditing, and customer satisfaction. We previously suggested keeping your eyes wide open for metrics of all sorts: the same applies to measurement methods.

Tip: Whereas factors of this nature may be of greater concern as your *information security measurement system* matures, the basics are worth considering even at the start of your metrics journey. Look for opportunities to try out creative approaches and develop your own skills as a metrician by actively developing and using different measurement techniques. Aside from anything else, variety helps reduce the cynics' "Oh no, not another survey!"—which tends to lead to careless or dismissive responses.

Similar considerations apply to the use of surveys, interviews, and other methods because they also involve a variety of approaches with differing costs and benefits. Professional metricians may be concerned with the precise wording of questions in a survey or questionnaire, for instance, as well as their presentation, the preamble, any inducement to respond, even the sequence of questions posed. Designing questionnaires and interview situations to avoid bias involves both art and science.

11.1.4 Online or In-Person Surveys

As modern information security professionals, we naturally lean toward using online (computerized, generally Web-based) survey techniques for gathering responses from people, but that is not always entirely appropriate. Online surveys have the obvious advantage of being relatively cheap and easy to conduct, but that might be considered a drawback if it encourages us to develop them on a whim instead of thinking more carefully about what we are aiming to achieve and how best to do it.

Measurement methods that involve people—metricians—gathering the raw data have a number of plus points, particularly when measuring other people. A human metrician

- Can introduce and explain the exercise, reacting dynamically to the respondents' queries or obvious difficulties or concerns concerning the survey, the questions, anonymity/privacy, etc.
- May select particular respondents dynamically, for example, to satisfy a pre-defined quota of males versus females, staff versus managers, keen versus reluctant respondents, etc.*
- May make notes about respondents that they might be unable to identify or reluctant to admit (e.g., social status, attentiveness, and intellectual capacity).

* While the quota approach introduces obvious concerns about the randomness of the sample, don't forget that online surveys tend to favor computer literate respondents with the time and the inclination to respond.

Tip: Given the cost differential, hold in-person surveys in reserve for those situations where the human interaction will enrich the responses beyond what a machine can reasonably achieve, and be careful about who you choose to conduct them. Customer satisfaction surveys are an example: customers may be more likely to open up honestly to a friendly, receptive, personable, human interviewee, especially a dispassionate third party, than to a cold, hard, logical computer system. Most of us can express ourselves far better in person than online, especially given the confines of the usual online survey methods. If handled well, a metrician's reaction to the responses may even defuse awkward situations and make respondents feel their opinions actually matter—a cathartic, positive experience in its own right.

11.1.5 Scoring Scales

Anyone who has been asked their opinions on a street corner or telephone survey should be familiar with Likert scales, more accurately known as Likert items after psychologist Rensis Likert's work in the 1930s. Likert items are used to score a respondent's opinions in terms of their bipolar direction (positive or negative, like or dislike, etc.—generally symmetric or balanced about the center point) and extent ("strongly like" is more extreme than plain "like").

Whereas Likert items offer respondents discrete choices (typically 5 or 7 points*), continuous scoring scales extend the idea by allowing even finer discrimination (e.g., percentage scales with at least 101 notional points), although they require greater thought from respondents to generate accurate results (Figure 11.1).

These three examples of continuous scales, along with others throughout this book, illustrate how to get more complex proportional data from questions or

Tip: Where possible, it helps to encourage respondents to explain their chosen scores, particularly if they are extreme, counterintuitive, or provocative. A simple way to do this is to provide a blank space for comments or notes underneath the scoring scale with its criteria—see the sample opinion survey form in Appendix D for an example. With this approach, you can gather textual responses, anecdotes, and impressions as well as numeric metrics.

* Opinions vary on the merits of providing a central "undecided" option. Some lay people are *adamant* that it is better to force undecided respondents to choose one way or the other by presenting an even number of choices, but whether that really does force respondents to choose rationally, to pick an option at random, or to skip a question entirely is not completely clear. All we will say is that most professional metriicians prefer odd-numbered choices.

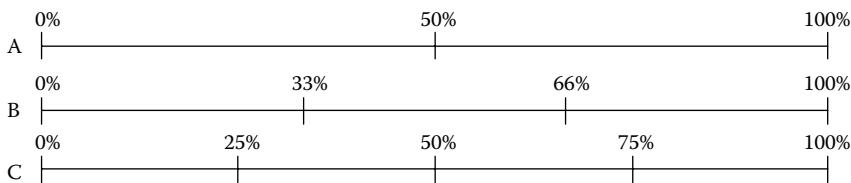


Figure 11.1 Continuous scoring scales.

situations that don't necessarily beg such simplistic responses. Scales A, B, and C would normally, in practice, be supported by three, four, or five descriptive criteria, respectively, stating what each of the identified scoring points means or implies. However, respondents are not forced to select those specific scores—they can interpolate by marking the line at the most appropriate point even if it falls between the identified marker points.*

Generally speaking, as we use them to measure information security, 50% marks the boundary between whatever is being measured being considered acceptable or unacceptable by the respondent; 0% means absolutely terrible, outrageous, a total disgrace, and 100% goes beyond fully acceptable and good practice into the realm of best practice.[†]

Continuous scales benefit from thoughtful design and use, so they tend to work well in a professional environment where respondents have the mental capacity and application to interpret the questions and criteria sensibly. However, provided the questions and criteria are reasonably clear and sufficient responses are gathered to even out statistical anomalies, even off-the-cuff responses or first impressions may be enough to generate scientifically valid data.

11.1.6 Audits, Reviews, and Studies

In addition to metrics associated with operational processes, metrics may be gathered by discrete, sporadic, ad hoc, or indeed regular audits, reviews, and studies of

* Continuous scales are not quite so easy to computerize as the simple radio-button five, seven, or nine-point Likert items, but it can be done. Some Web programmers even use fancy sliders and other visual cues to make them both intuitive and interesting.

[†] Theoretically speaking, the scales extend below 0% and above 100% because it is conceivable that a respondent may feel a given situation is even more dire than the appalling criteria stated at 0% or exceeds what would normally be considered a tough stretch target at 100%. This makes sense as information security is described by the likes of Donn Parker as an “unbounded problem space.” Ideally, such extreme scores should be discussed with the relevant respondents, leading to further insight. If you develop the facility to gather and analyze scores from such continuous scales, do allow for scores that are below 0% or exceed 100%, rare though they may be.

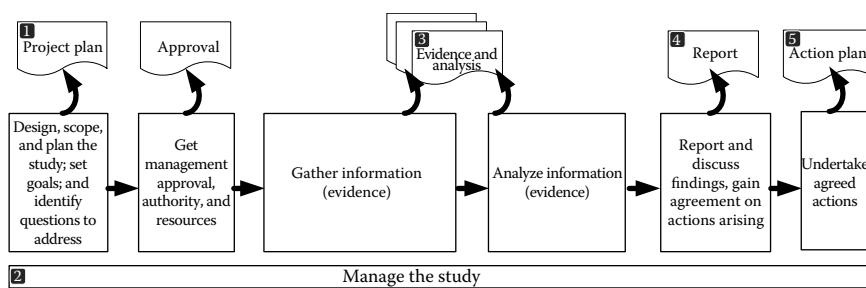


Figure 11.2 Typical audit/review/study process.

various kinds. Typically, these will be looking into and dealing with something of interest or concern to management.* The approaches vary in detail, but, in general, they include activities along the following lines (Figure 11.2), generating at least five types of metric as numbered and described below:

1. A well-written project plan for the study will state a number of key study parameters (such as resources required and timescales), which can be used to generate project-related metrics.
2. As the study progresses, conventional project management activities will use project metrics to track and control the status of the project (such as actual versus planned expenditure).
3. The information/evidence and analysis generated by the study will often include measures of the subject of study (e.g., the number of inadequately treated information security risks in the area).
4. Management reports often incorporate metrics in the form of tables, graphs, ranked lists, etc.
5. Action plans can also include or be used to generate metrics concerning the status of the agreed actions or outcomes of the study (e.g., completion delayed or on time).

11.2 Data Analysis and Statistics

To repeat, this is not the right book for you if you are seeking detailed advice on analytical and, especially, statistical techniques: there are plenty of other books and mathematical resources that do a far better job in this area than we could hope

* Hayden (2010) is strong on the metrics associated with security measurement projects.

to achieve.* However, we cannot escape without offering a very brief, high-level overview of some of our favorite techniques.

Counts and rates: how many items fulfill the criterion or criteria applied, often within a stated period. Simple counter metrics (such as the number of IT systems that have been fully patched) are generally cheap to collect but offer limited value. Counts may be useful, for instance, for planning operational activities (e.g., if you know how many IT systems there are in total, subtracting the number that have been patched tells you how many have yet to be patched, which can help in planning the resources needed to do it). Similarly, historical rates (e.g., the average number of systems patched per day) give management a clue about future rates (e.g., how many systems are likely to be patched in the coming week) and provide a handle on management activities (e.g., assuming the number of people assigned to patching is the main limiting factor, we might expect to halve the amount of time taken to patch all the remaining systems if we double the size of the patching team).

Cumulatives: cumulative counts recording how the total count of items has grown (accumulated) during the period leading up to today (usually). Cumulatives are commonly used in the analysis and presentation of financial expenditure and income, for example, showing how the total expenditure on security consultants has grown month-by-month during the year to date. Provided the curve is increasing fairly evenly (in other words, if the trend is clear), it is simple to *estimate* the total values in successive future months (although things may still change unexpectedly: prediction is inherently uncertain). However, if the curve increases in fits and starts, future values can only be guessed at best (predictions are largely pointless in this situation, having a very high margin of error).

Arithmetic mean or average: calculated as the sum of the values divided by the number of values summed. The mean value is considered typical for evenly distributed values. For skewed distributions, however, with a long tail of high (or low) values, the mean may be atypical, moving away from the median value (see below) into the tail. Means are simple to calculate and widely used, although the term “average” is used in common speech. Considering a single, representative mean value is easier than having to try to describe the actual range of values.

Median (as in median line): the center of a set of values ranked or arranged in order from lowest to highest value. The median value is more typical or representative than the mean of a skewed data set. Half the values will be greater and half less

* Being pragmatists, we manage quite well with these rudimentary techniques thanks to spreadsheet software, Google, the odd statistics textbook, and, on occasion, assistance from a passing expert. Seldom have we met managers with the skills to challenge our analyses, which is really a sad indictment of management: one would have thought that because organizations run on numbers, those in charge would have a very solid understanding of mathematics and statistics. In practice, numbers without dollar signs might almost be invisible.

than the median or middle value of the set. Tracked over time,* both means and medians even out short-term fluctuations and so indicate trends. Spotting a trend toward criminal hackers increasingly using Trojans to compromise inadequately secured PCs of customers, for instance, a bank might decide to put more resources into its customer-facing security awareness program, supplementing its back-end fraud control systems.

Standard deviation and variance: along with *statistical tests*, such as chi-square, student's *t*-test, and ANOVA, measure the amount of variation between members of a set of values, such as successive measurements of a single security metric (e.g., the number of virus incidents per month). Generally speaking, if all the measurements are closely clustered around either a single value (like tightly grouped holes on a shooting target) or closely follow a line on a graph, they are considered an accurate representation of whatever is being measured. If the measurements are widely distributed, however, they may bear little relation to the actual value being measured because, perhaps, of random variation in the actual value or errors in the measurement process (typically a result of their being other relevant factors that are not being measured or controlled): in short, they are considered relatively inaccurate. Such analysis may be useful to compare different metrics or measurement techniques or to decide how much faith to place in a single one. Given enough measurements, the more advanced statistical techniques can give greater insight into a metric provided they are correctly calculated (which is not that hard to do—simply process the values through the appropriate formulae) *and* correctly used (which is harder to ensure as it takes statistical expertise to appreciate the purposes and limitations of various statistical techniques).

Distributions: generally displayed as curves on graphs relating measurements or counts of items (on the vertical *y*-axis) for each type of item (on the horizontal *x*-axis). While the curves are quite pretty to look at and can be used to measure off values, the real power of distributions arises from the associated mathematical properties. The two most common and useful distributions are the following:

- *Normal:* the normal or Gaussian distribution gives the well-known bell-shaped curve. The curve is symmetrical with the mean value in the center of the bell. The bulk of the items cluster around the central part of the curve: if the distribution is truly normal, nearly 70% of the items are within one standard deviation of the mean value, and approximately 95% of the items lie within two standard deviations of the mean. The remaining ~5% of items more than two standard deviations from the mean form tails above and below the central bulk. The mean and standard deviation are quite easily calculated

* A rolling average is similar in that we calculate and plot the mean or median of the last *N* measurements, where *N* is less than the all-time total number of measurements taken. It is another way to smooth out the peaks and troughs.

from a list of values. Both values are needed to describe a true normal curve mathematically—think of them respectively as the horizontal position of the bell on the x -axis and the width of the bell.

- *Poisson*: the Poisson* distribution typically reflects the number of events (such as security incidents) that happen during different periods (such as months or years). If the mean rate of events is low, the distribution is skewed toward low values with a long lingering tail of higher values. If the organization suffers, say, one hacking incident every two months on average (a rate of half an incident per month), most months will tend to have no hacking incidents, some will have one, fewer months will have two incidents, and in really bad months, there may be three or more incidents. If the mean rate is higher (e.g., five malware incidents per month), the distribution becomes less skewed and more symmetrical with tails on both the low and high sides, looking more like the normal curve, in fact. The mean (average) rate is enough to describe a true Poisson distribution mathematically.

Metrics aggregation: can involve additional analysis using historical values for one metric or comparing and contrasting values from several metrics. Related metrics concerning different aspects of a subject area can be used to build up a picture, such as using metrics on exceptions, exemptions, incidents, and enforcement activities to establish the organization's status on security compliance.

Trends: about projecting or predicting values into an uncertain future based on past data and the current trajectory. Humans are quite adept at seeing patterns of this nature, but there is a danger of projecting too far as a result of inaccuracies and variance inherent in the preceding data and nonlinear relationships. Statistical trends analysis can only help up to a point: those interpreting and using metrics must be wary of seeing and acting on trends that turn out to be false, hence the need to continue collecting measurements once trends are identified. Projection gives a best estimate: measuring what actually occurs against the prediction tells us how accurate our prediction was, which can be useful for further metrics development. Outliers—measurements that appear significantly different from the trend—complicate trends analysis: if an outlying value appears, are we looking at the start of a new trend or merely a random fluctuation that will even out in time? The consequences of making significant decisions may be disastrous or fortuitous depending on whether the outliers are above or below the line, but occasionally, we may be forced into making security management decisions that turn out to have been inappropriate—such is the nature of risk.

* Poisson is French for fish, representing the curve with a fishy tail.

Correlation and regression analysis: techniques that help us identify relationships between multiple factors that may *appear* to be linked.* While keeping other factors constant, as one factor is moved or altered, a correlated factor moves in synchrony either in the same direction (positive correlation) or oppositely (negative correlation). This kind of relationship *appears* to indicate what we call cause and effect (if we go faster when the lever is moved up, the lever appears to be an accelerator), but correlation alone is not proof of this (perhaps the lever is on a ship's bridge, connected to nothing but an indicator in the engine room where engineers control the ship's speed manually; conversely, perhaps the lever is, in fact, connected to the brakes, and we go faster when the lever is raised because we are on a hill!). Statistical techniques can also identify weak correlations, meaning mathematical relationships that are far looser or weaker and difficult even to visualize on a graph, and regression analysis can determine apparent linkages between multiple factors. Correlation and regression analysis can be an important source of clues about possible causal relationships in topics as complex as information security, where we cannot control and may not even appreciate all the factors involved.[†] Statistical analysis of substantial security metrics data sets (one form of data mining) may identify correlations that were previously unnoticed. That, in turn, may lead to new insights into security, perhaps even causative relationships.[‡] Such correlation and regression analyses fall into the realm of advanced metrics, however, because most organizations currently fall well short of even the basic level of metrication we have mostly discussed.

Emergent properties are exemplified by the perfect storm, an incident or disaster caused by a number of lesser events collectively resulting in a much more extreme outcome than could have been foreseen or planned for. Such extreme events could be the result of either a single unknown threat vector simultaneously exploiting a set of otherwise acceptable risks resulting in a calamity or perhaps a number of threats all materializing simultaneously, breaching a number of unrelated vulnerabilities

* Metrics based loosely on the principle of correlation are generally known as indicators because they are merely indicative of, rather than directly associated with, the subject of measurement. Only proper statistical analysis can determine just how indicative they really are.

[†] Correlated events are often mistaken for true causal relationships, especially when the correlation appears strong. For example, just because the boss *always* takes a big dose of antacid whenever the network is down doesn't mean taking antacid causes network outages! Nor do network outages literally cause the boss to consume antacid through some form of mechanical linkage. More likely, the inability of the boss to handle stress is one causative factor, although even that is probably not the root cause. His or her upbringing and general disposition are probably relevant. There might even be genetic factors at play. Perhaps he or she takes antacid at other times that we don't even notice.

[‡] There are dangers in *assuming* causative relationships between two factors without identifying a credible linkage, particularly if the correlation is not strong. There may be other, far stronger factors involved, but, during the period of analysis, they either haven't been tracked or they have been stable and, therefore, did not affect the observed changes.

Tip: Don't try to run before you can crawl. Not only are advanced statistics tricky to apply correctly, they are likely to pass over the heads of the people to whom they are presented. Complex analyses may be entirely appropriate in certain limited circumstances, but concentrate on getting the basics right first, and the rest will follow. Don't neglect the Meaningful PRAGMATIC criterion. Fancy metrics that are hard to fathom are unlikely to resonate with the audience and may be treated very cynically.

that otherwise individually appeared to pose an acceptable risk.* Emergence could also involve an overwhelming manifestation of a new technology that renders existing security controls outmoded, bringing up the mathematical notion of chaos theory—a fragile system that can suddenly flip to an alternative mode of operation (e.g., the trusted systems administrator who suffers some sort of personal crisis and becomes a saboteur).

Normalization: systematically adjusting data values to a common basis of measurement—measuring things on the same scale, as it were, or reporting them on the same basis. Normalization may be necessary, for example, when the analytical calculations for a security metric are changed for some reason: values prior to the change (if still available) can be recalculated using the new calculation and restated in order that historical comparisons and trends will remain valid.

11.3 Data Presentation

11.3.1 General Considerations

There is an art to presenting metrics in such a way that the audience first understands the true or rather the intended meaning and, second, is motivated to act appropriately. This issue goes beyond the science, the mathematics, and the data

Tip: How exactly *is* the CEO expected to react when presented with a Nessus scan showing 472 open vulnerabilities in Dayglo yellow or bright red? Consider your audience. Make their jobs easier.

* Metrics measuring an increase in the background radiation level in information security may give an indication of a storm brewing—for example, an increasing number of malicious packets being rejected by the firewalls *may* foreshadow an imminent network attack. The trouble is that many other situations (such as changes in network topology or firewall rules) can also boost the packet rejection rate, so such metrics must be treated with caution.

into the realm of comprehension, impact, art, and even passion. It is complex, too, involving factors, such as the following:

- *The audiences*: who they are, their perspectives, and their personal preferences in terms of presentation styles, amount of information, depth of analysis, etc. (see Chapter 4).
- *Conventions*: the way other metrics and information gets presented to management inevitably sets expectations.* Are things generally presented to management in neatly printed and bound reports, through audiovisual presentations, through the intranet, or by some other means? Is it normal to use color? What about diagrams, graphs, and figures as opposed to or in conjunction with words?
- *Topicality*: what is currently relevant and of concern to management. If management is strongly focused on *compliance*, then be sure to include it. If *risk* is this month's burning hot topic in the C-suite, you'd be nuts to ignore the opportunity. If *value* is so last year, move on or, at least, find a different term for it!
- *Cost*: including not just your time and effort needed to gather, analyze, and massage the figures into pretty charts but for the recipients to extract their intended meaning.
- *The organizational and business context*: is now a good time for the audience to focus on information security matters, or are there more pressing issues, making this something of an annoying diversion? There is a natural temptation to want to present the latest report or recommendation as soon as it is ready to go, but sometimes we would be better off biding our time for a more suitable opportunity, such as following a related incident or near miss when the material will have greater impact.
- *Cultural factors and collective biases*: staying on message, toeing the party line, etc. Bias in reporting and interpretation of metrics is an extremely important topic in its own right. Please take a look at Appendix J.
- *False consensus*: the technical name for yes men agreeing with a senior.

11.3.2 Analytical Tools and Techniques

We have already discussed the statistical element of data analysis, but there is more to it than that. Competent analysis of the statistics draws out the key aspects, issues, concerns, and lessons for the future. It breathes life into the numbers. Most

* Being aware of conventions does not necessarily mean we have to follow them. There are situations in which it pays to take a different route, deliberately. The way in which a message is put across may give it additional impact, but equally, it may be too radical for some. In other words, there are both risks and opportunities in being unique.

Tip: Don't lose sight of your metrics goals. Dashboards may look pretty but unless the data are genuinely of concern and value to management, resist the urge to present them and add to the noise level.

importantly, it helps the audience understand and appreciate the real meaning of the metrics in business terms, which is, after all, the reason we go to all this bother.

As for tools, PC spreadsheet products, such as MS Excel, are perfectly capable of analyzing and presenting information security metrics for all except perhaps the largest, most metrics-intensive organizations. Basic sorting, mathematical, statistical, and graphical functions are invariably provided, while add-on analytical packages, such as those often used by auditors and scientists, can be useful for metrics purposes, too.

Spreadsheets lose their edge when conducting advanced statistical analyses, especially on large data sets, such as historical comparisons over a long period. Dedicated statistics or database programs take more effort to understand and configure but may make it easier and quicker to come up with the right answers.

Sometimes analytical and reporting functions are built in to IT systems and application software, so it's simply a case of screen-grabbing the output graphics or exporting the data tables to your analytical and presentational weapons of choice. Most, if not all, enterprise security management systems incorporate some sort of executive dashboard affair, which (despite the name) generally offers operational metrics of interest to the security professionals using and managing the systems rather than to senior managers.

Other standardized forms or styles of analysis also have their place in written reports and presentations, for example, SWOT (Table 11.1).

PEST follows a similar format to SWOT, but the respective categories for analysis and reporting are political, economic, social, and technological.* RACI charts are somewhat different; however, these identify who is responsible, accountable, consulted, and involved, usually at various stages of an important business process.[†]

Deductive reasoning builds an argument or prediction on the basis of a series of known or likely relationships (e.g., given that lengthy, complex business continuity plans are relatively awkward and costly to maintain, we deduce that plan length and complexity is probably inversely correlated with plan integrity and quality). Deductive reasoning has obvious application in designing metrics to test

* There is nothing particularly magical about SWOT or PEST, by the way; they are merely commonplace management reporting conventions that conveniently remind us to cover the respective conceptual areas. Given that they both divide the topic into four distinct categories, they bear a superficial resemblance to the Balanced Scorecard (Kaplan and Norton 1996).

[†] Explicitly distinguishing responsibility from accountability is a major advantage of sound RACI analysis.

Table 11.1 SWOT Table Example

<i>Strengths</i>	<i>Weaknesses</i>
<ul style="list-style-type: none"> • List the positive aspects here, one at a time as separate bullet points. • The left hand boxes help to balance out the negatives over on the right. • When discussing or presenting the SWOT, start in this box, then move on to the weaknesses, then the opportunities, and finally end with the threats. 	<ul style="list-style-type: none"> • List the negative aspects and drawbacks here. • The upper two boxes tend to be historically focused, covering prior and possibly current issues. • Try not to go beyond five points in any box: the SWOT format is ideal for highlighting and summarizing just the key points, not to squeeze an entire thesis into each box (this mult clause point is too long, in fact, and should be shortened and simplified).
<i>Opportunities</i>	<i>Threats</i>
<ul style="list-style-type: none"> • Identify business opportunities here, situations where additional business benefit can be obtained with relatively little outlay. • Remember that security exists to support the business, not the other way around. • At a push, identify opportunities for improvement, but try to maintain a positive attitude. 	<ul style="list-style-type: none"> • Highlight threats (and vulnerabilities, exposures, impacts, or risks) of concern here. • The lower two boxes tend to be forward-looking, projecting things into the future. • Because you discuss this box last, you will probably leave the audience with a lasting impression of the threats, hopefully enough to stimulate them into action.

such hypotheses. In contrast, *inductive reasoning* involves drawing conclusions and inferring relationships as a consequence of observations and measurements made (e.g., the integrity and quality of departmental business continuity plans decline as they become longer and more complex, presumably because they are relatively awkward and costly to maintain). Inductive reasoning has obvious application in making sense of the measurements. Deductive and inductive approaches are complementary.

11.3.3 Reporting Tools and Techniques

Word processing packages, such as MS Word, and graphical/presentation tools, such as MS PowerPoint and MS Visio, contain lots of functions to help you turn

Tip: Take the time to learn how to use Word's styles and use them consistently for a more professional look. In this book, for instance, the same formatting is applied to all these tips simply by defining a style called "tip" that automatically applies the correct font, size, borders, shading, line/paragraph spacing, etc. when it is applied to a paragraph of text. If we decide to change the look of the tips, we alter the style once to make the change simultaneously to all 150-odd tips in the book. Headings, body text, captions on figures, and footnotes are all handled in the same way.

a somewhat disorganized pile of spreadsheet tables and graphs into a structured, coherent, informative, and motivational report and presentation.

As with presentations (see below), management reports should tell a story, meaning that they need to be planned and constructed as a whole, using the metrics to illustrate and draw out the key points along the way. "Illustrate" is an important term: stick to graphs, diagrams, and 'top ten' lists wherever possible in the body of a report, relegating detailed data tables and complete lists to the appendices for readers who feel the need to explore them.

Being able to write clearly and professionally is an *essential* management skill, particularly when using metrics for management information. All worthwhile metrics tell us something we need to know, but often the message needs to be pointed out, especially the first couple of times a new metric is reported or presented. The trick is to help the audience glean the meaning, the interpretation rather than the actual data. If you phrase things in business language rather than technical terms, so much the better. Compare these two example paragraphs, both reporting on the same graphical metric (Figure 11.3):

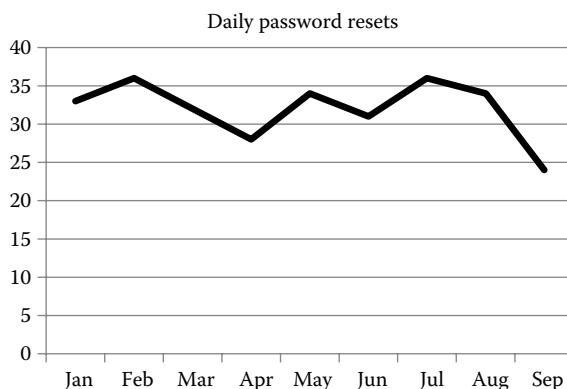


Figure 11.3 Example graphical metric.

Tip: Word's templates make it easy to generate standardized management reports with the same overall layout, structure, look, and feel each time. After having crafted your first metrics report in a regular series, save it and then go back through it to erase all but the standard boilerplate text and placeholders for the data tables or graphs, saving the skeletal version as a Word template. Start constructing subsequent reports using the saved template, updating and resaving the template if you need to change the boilerplate or formatting.

As you will see (Figure 11.3), the number of password resets has reduced from approximately 34 per day last month to approximately 24 per day this month. We attribute the 10-point reduction in the level of resets to a security awareness initiative on passwords that took place during September. The rate had been as high as 36 resets per day previously.

Last month's security awareness initiative gave employees tips on choosing more memorable passwords. The number of password reset calls to the help desk was markedly reduced as a result. With each call costing about \$15, we estimate this is saving \$3000 per month.

11.3.4 Presentational Tools and Techniques

PowerPoint presentations are much maligned, but the reason has far more to do with those who develop and present the material than with the product. Overuse of excessively terse bullet points is an obvious issue along with the opposite problem—stuffing slides with far too many words and using far too many slides in presentations. There are plenty of sources of advice on making better presentations, so we offer only a few key points here.

Tip: It is probably clear from previous comments that we have severe misgivings about so-called management dashboards and executive information systems. Most seem to major in presentation gloss and blinkenlights rather than substance. Do you honestly think your managers will be taken in by a set of fancy Flash graphics if the metrics being reported are not PRAGMATIC? Don't fall for the metrics dashboard vendors' sales pitch if that means neglecting the quality and integrity of the underlying data, the analysis, and, of course, the resulting metrics. Experienced managers may be cynical and question the expense on such systems, especially if they have the sense that the metrics are not entirely PRAGMATIC.

Tip: Focus, *focus, focus!* You are far more likely to hit your target if you actually know what it is that you are aiming for.

Above all, think about what you intend to achieve through a presentation. Are you aiming to provide information, gather information, stimulate discussion, entertain and motivate the audience, highlight certain points, explain complex metrics, gain agreement to actions, or something else? Sure, most presentations have several such aims, but which one or, at most, two are crucial? Absolute clarity on this makes a difference to the way you design and present the material.

Leave most of the words to the presenter: slides are good for color graphics, graphs, diagrams—conceptual representations (such as mind maps) that the presenter can explain verbally in person. Don't, however, take that as a license for the presenter to overwhelm the audience with a full-on stream-of-consciousness flood of verbiage. Speak relatively slowly, all the time watching and reacting to the audience. If they seem to be bored, move ahead more quickly. If they are looking lost or puzzled, slow down, explain more carefully, and ask them questions to gauge their comprehension.

Tell a story. Before you even open PowerPoint to start composing, be clear in your mind about the key message or messages (seldom more than two or three) you want to put across and remind yourself about why those messages are important to the audience. Start with some introduction or context setting, and then, in successive slides, lead the audience through a connected sequence of thoughts leading to a logical conclusion. When planning a new presentation, figure out the storyboard first, putting a few markers in place to let the audience know when you are moving

Tip: Watch stage acts, such as stand-up comedians, magicians, and evangelists, for tips on keeping the audience totally focused on the presenter. Notice their sheer physical energy, the passion, the dramatic pauses, and enhanced facial expressions. Notice how little of the act concerns the actual words. We're not suggesting that you slice your stunning assistant in half with a huge sword during a management presentation, just that you make an effort to bring your presentations to life and make them enjoyable as well as effective—in fact, we are convinced those factors are closely correlated. If your presentations always fall flat, it could be that you or your materials are simply not stimulating enough. Try being more upbeat and enthusiastic, more animated, more contentious or outspoken, more in tune with the audience—whatever it takes really to get a positive reaction.

Tip: Make a real effort to solicit candid feedback from your audience or from experienced colleagues concerning your presentation style, especially if you are a novice. Keep notes on things that worked well and those that didn't quite go as planned. Practice hard by presenting as often as you can and watching how others do it.

between discrete sections. Give the audience some sort of map or outline of the presentation using section headers or separator slides to let them know when they are moving out of one area into new territory.

If your presentation builds up a complex picture slide-by-slide (which is a technique that works well for us, for example, working successively around the arms of a mind map diagram), minimize or gray out the previous details as you expand on each new area in order to reduce distractions. End with the full picture in all its glory, giving the audience time to let it all sink in and then discuss the presentation. The discussion is a vital part of the communications process, both in terms of ensuring that the audience understands and, we hope, accepts the information presented and in moving them on to the next stage, which usually involves outlining an action plan and assigning responsibilities for actions arising to the relevant functions or people.

Don't read aloud the actual words on the slides. It is demeaning, in effect telling the audience you don't trust them to read for themselves. Use the slides as prompts for the presenter to elaborate on topics of interest and concern. PowerPoint's speaker notes are an ideal way to provide additional information or reminders for presenters who are not entirely familiar with the content, and they make usable handouts, too (under "Slides" in the print dialogue, select "Notes pages").

Make presentation sessions as interactive as possible—not just an outpouring of information from the person at the front to the sea of faces in the audience but an exchange of information (albeit a lot of it nonverbal). Think seminar not sermon. Actively invite and address questions from the floor during the presentation when thoughts are still fresh in their minds, and where appropriate, refer back to queries or comments when discussing later slides. Work with your audience: they will

Tip: If possible, try to involve the presenter in designing and preparing the slides and speaker notes. It can be hard to speak convincingly to someone else's presentation, especially if the content is unfamiliar. At the very least, ensure the presenter makes time to go through every slide, rehearsing the messages and thinking about particular aspects to point out.

Tip: If your time management is weak, try to cover the most important messages early on in case you run out of time later.

respond if you apologize for cutting the discussion short in order to push ahead, but always try to leave time at the end to go back to points of concern. Don't be totally obsessive about your timeline as it is better to communicate a few key points well than to skim so fast that nothing sinks in.

Use props to highlight key data points, trends, etc. Recount anecdotes and quote comments gathered during the course of collecting and analyzing the metrics data, including poignant observations from people in the audience if they are already aware of the content.

Keep unnecessary animations and especially whizzy sound effects to a minimum. Displaying bullet-point lists one dreary bullet at a time can be painfully tedious and often distracts the presenter from focusing on the audience.

11.3.5 Graphs, Figures, Diagrams, and Illustrations

Metrics are normally stored and analyzed mathematically in the form of lists or tables of numbers, but thanks to our innate human ability to recognize visual patterns, most people get much more meaning if the metrics are presented graphically. The following descriptions and examples illustrate the most common, and a few more, creative graphical designs.*

The graphs we see most often are called *line graphs*. A typical example was shown earlier in Figure 11.3. Line graphs are good for displaying successive data points over time, either using straight lines to connect the data points, trend lines (plotted

Tip: Regardless of what software packages you use, they are, of course, just tools whose effectiveness is largely down to you, the user. Don't let your fascination with analytical and presentational technologies overshadow your analysis of the information and the audience's capability to understand the metrics.

* While not exactly metrics, we have included a number of *mind maps* in this book because we find them useful, both to get our thoughts in order on complex issues and to put them across to our readers in a structured way. We use them for seminar presentations too, working around the arms of the mind map in successive slides. Mind maps can get a lot more colorful and creative than the monochromatic ones here. If this idea intrigues you and suits your style, read anything by Tony Buzan for plenty of inspiration along the same lines.

Tip: There are many formatting options for line graphs and, indeed, all the others described here, but be sensible about it. Develop and stick to a relatively simple, consistent style, preferably one that works in monochrome if your audience mostly uses monochrome printers or photocopiers rather than PC displays or color prints.

using appropriate correlation statistics), or, for sheer ease of use, the smoothed line option in Excel to even out the fluctuations and emphasize more significant trends (Figure 11.4).

A big bold title, good-sized text, and quite thick lines make the graph easy to understand at a glance. The horizontal lines across the chart area, plus vertical lines in some cases, help the reader identify relative values (e.g., showing clearly that the Sep data point is lower than the dip in Apr in our example).

Line graphs can, of course, display multiple ranges of values against the same *x*-axis (horizontal, which is usually but not necessarily time related), typically distinguishing each line by its color or style (e.g., solid, dots, or dashes) and width. Displaying two distinctly different ranges of data values on the same graph is easier using separate *y*-axes (vertical) on the left and right sides of the graph, respectively, or using logarithmic rather than linear scales to compress high values.

Individual data points can be identified with markers or their values, although, for most purposes, it is simple enough to read values off the appropriate axes. The axes should also be labeled if there is any doubt about their meaning. A key is helpful to explain what each of the lines is on multiline graphs, placed somewhere outside or even inside the chart area or using text labels pointing to the lines.

Bar charts are best suited to displaying data values belonging to discrete/discontinuous categories, for example, the number of information risks in the inventory, classified by their significance (Figure 11.5).

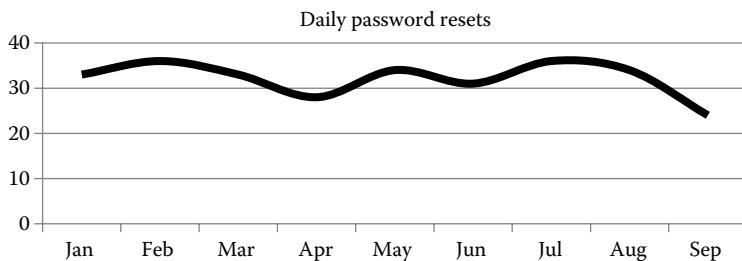


Figure 11.4 Example of smoothed line graph.

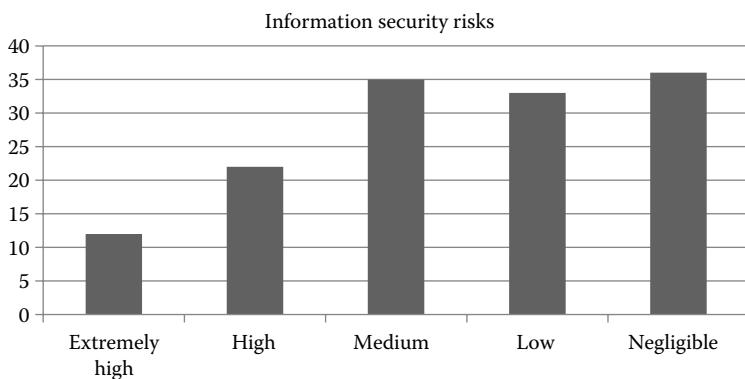


Figure 11.5 Example of bar chart.

Try to place the categories in a sequence that makes sense to the viewer, for example, sorted by the nature of the category (as in this example) or by the data values (for ranked data sets).

Pie charts are great for showing proportions of a whole, for example, the percentage of system accounts that are unprivileged, privileged, and noninteractive (Figure 11.6).

In order not to distract attention from the larger and usually more significant values, it is common practice to group smaller values together under an “Other” category.

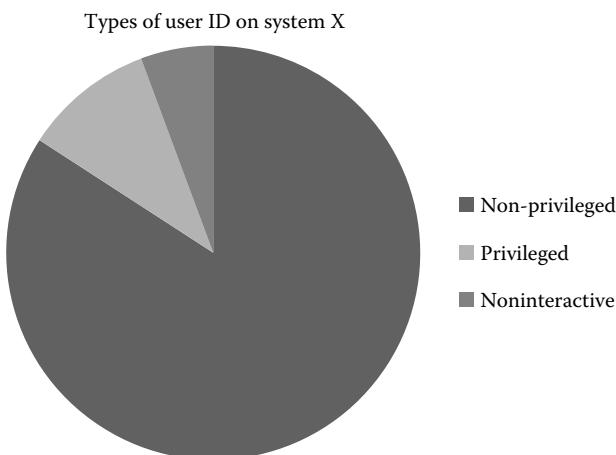


Figure 11.6 Example of pie chart.

Tip: Instead of presenting the key as a list as shown in Figure 11.6, it may be better to use text labels pointing at each slice of the pie, especially if there are several slices that are hard to distinguish by color or shading.

Area graphs are used when the area under the curve is more important than the curve itself, for example, to display cumulative values changing over time (Figure 11.7).

Spider diagrams/radar charts have approximately 10 axes, arranged radially from a central point in a sequence that makes some sort of sense. Connecting the data points between successive axes produces a spiderweb effect. Coloring the area under the curve produces the example shown in Figure 11.8, such that relatively high or low values in one part of the diagram produce an obviously lopsided image.

Scattergrams plot individual data values scattered across a plain x - y graph surface, showing any clusters or outlying values (Figure 11.9).

This example of a scattergram divides the graph area into quarters according to the scales. Arguably the magic quadrants and similar two-by-two matrices much loved by MBAs and consultants have passed their sell-by date, but in this example, the three departments whose transaction and error numbers put them in the top two quadrants could probably learn something from those in the lower quadrants, particularly the finance department who one would naturally expect to lead the way.

Fancy *three-dimensional graphics*, especially in color, can add a bit of gloss to an otherwise drab report and may be used to emphasize certain facets of a data set (e.g., using a raised perspective viewpoint to make high values stand out from lower ones). However, they can also be distracting and even misleading (e.g., if values

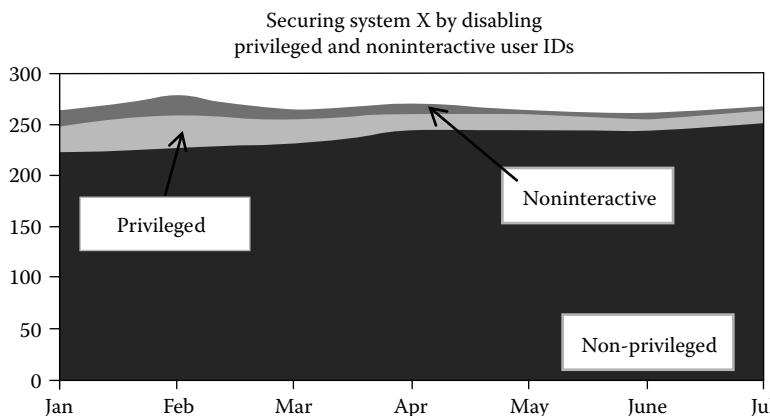


Figure 11.7 Example of area graph.

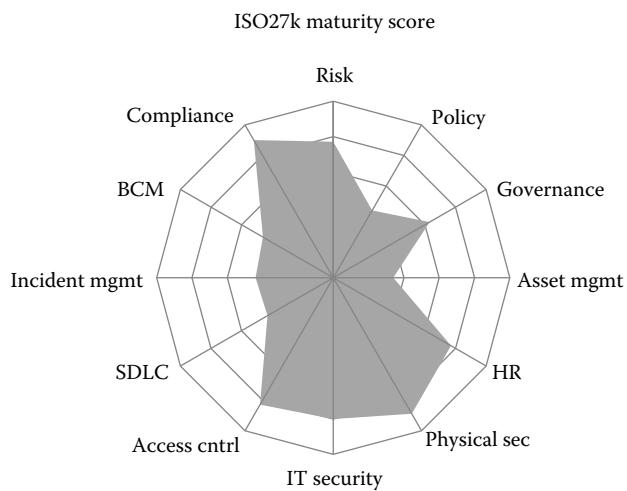


Figure 11.8 Example of spider diagram/radar chart.

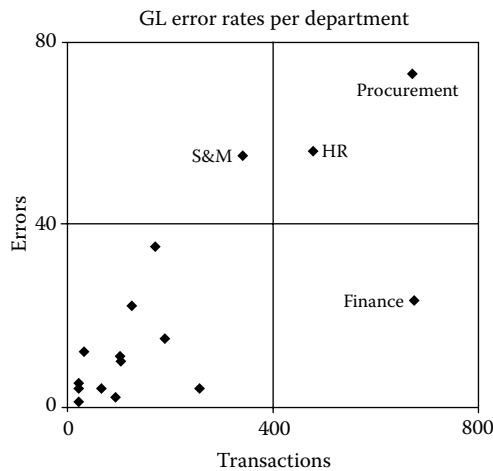


Figure 11.9 Example of scattergram.

nearer the viewer obscure those behind). It's best to use them sparingly, probably not in regular daily, weekly, or monthly reports but perhaps to make annual reports more attractive.

Venn diagrams are a way of representing sets or groups of items that overlap to varying extents (e.g., Figure 8.2). Strict mathematical forms find limited application

in information security, but the general principle of graphically demonstrating intersecting or overlapping areas has more utility.

11.3.6 Drawing Attention to Specific Issues

It could be argued that metrics exist to identify particular situations, incidents, trends, or concerns. Sometimes they do speak for themselves, for instance, when major issues are self-evident. In most cases, however, the issues are more subtle, and many have to be pointed out to have any impact with the audience.

Color, size, and shape cues can all be used to emphasize certain data, trends, findings, issues, risks, etc. One example involves *x–y* scattergrams, where the physical sizes of the markers for the data points reflect their scale, in effect adding a third dimension to the graph.

Traffic-light reports (also known as stoplight charts) are widely used in management circles, but they are not universally appreciated: experienced executives profess little enthusiasm for them.* Nevertheless, there are applications where simply categorizing issues as high/medium/low and coloring them red/amber/green gives the necessary impact to the red ones and suggests the amber ones also deserve watching over. *Heat maps* apply the same simplistic logic, adding a color-coded overlay to stylized maps or diagrams showing the organization, its sites, departments, functions, processes, systems, etc., in order again to focus management's attention on the areas of greatest concern (see Figure 12.2 for a worked example). A heat map is an example of a metric that is neither a mono-dimensional number nor a two-dimensional graph. A well-constructed heat map is an information-rich format that achieves two important aims:

1. It allows for third or even fourth dimensions through the colors, sizes, nature, and number of overlays on the base map, along with the associated notes and narrative from whoever presents the heat map to, for example, a meeting of senior managers at the organization's security council or in a management report.
2. The semi-literal representation of the organization on the underlying base map and the accompanying notes or narrative are self-evident even to individuals for whom math is a black art. They can be visually intriguing, prompting management discussion and converting the bald information into understanding, appreciation, and, ultimately, knowledge that influences management decisions.

* In the main, successful managers have relatively high IQs and are perfectly capable of understanding quite complex data. Their intelligence is not really the issue, though—it's more a matter of them simply not having the time and inclination to delve into the details. Breadth of purview increases in line with seniority; hence, board members and executives have huge areas of accountability and responsibility.

Tip: It's easy to overlook this aspect of metrics. Good metrics, well presented, are stimulating and motivational. For some audiences and individuals, simple numerical or graphical metrics are boring, lifeless, and divorced from reality, whereas more creative analysis and presentation can bring the numbers to life and engage them in the discussion.*

* On the other hand, executives have been known to knock heat maps or traffic light reports as being too simplistic and coarse, some commenting that they can read stock charts for their stock options, so they can probably handle something a little more informative. It's a matter of personal preference and management culture, so finding out what the audience likes and dislikes is an essential part of developing effective metrics.

Textual *comments* and *labels*,* including asides, footnotes, or endnotes, all serve to point out items of interest or concern. Other techniques involve using pointers[†] or arrows, bolder fonts, highlighter, eye candy (bright graphics), and animation. If used judiciously, short, high-quality, audiovisual clips can make quite an impact in presentations. An example might be an animated time sequence showing how a certain metric (such as industrial espionage) has been gradually increasing for years but has suddenly escalated. Short, talking-head interviews with relevant experts, managers, or advisors can add interest and worthwhile content to presentations for managers and staff.

11.4 Using, Reacting to, and Responding to Metrics

The true value of metrics is in what we actually achieve with them, in terms of protecting and enhancing or improving the organization. Remember that dashboards, reports, graphs, heat maps, scoring scales, etc., and of course, the numbers themselves are merely tools. Being successful with information security metrics is not merely a question of putting information across but facilitating better manage-

* Take another look at Figure 11.9. Notice how, by labeling those four data points, the eye is naturally drawn to them, glossing over the unlabeled bulk of the data points in the lower left quadrant.

† Pointers are often literal in the case of in-person presentations: the presenter points at the display screen with a finger, a stick, or a laser pointer or turns to the relevant page of a report to show someone a key point buried within. Don't ignore such low-tech but dynamic techniques: they are often *more* effective than other methods.

Tip: The way in which security metrics are reported, presented, discussed, and explained has a substantive effect on how they are perceived by the audience. This is especially true when new metrics are initially introduced, particularly if they are not intuitively obvious, creating anxiety in both the audience and the presenter. As the audience gradually becomes more familiar with the metrics, the anxiety will diminish. Think about this issue *before* you launch a new security metric, and do what you can to knock the edge off those anxieties—perhaps chat about the metric beforehand with one or more friends from the audience, people who will give you honest feedback on it and can help deal with any pushback from their peers.

ment decisions and motivating people (managers and others) to act appropriately as a result of the information.*

Acting appropriately depends on the specific metrics and values, of course, but also the broader context. A significant security risk that would normally imply the need to implement different controls may be accepted by management, at least temporarily, because of more urgent priorities or to align with future plans. In the same vein, management may decide to address a bunch of related issues indicated by a number of metrics, even though the metrics considered individually may not be enough to prompt the action (e.g., a variety of metrics indicating long-term nagging concerns about security procedures, attitudes, and behaviors might be tackled as a whole through a joint initiative by information security and human resources).

Appropriate encompasses both the nature or type of response and its magnitude—in other words, good metrics drive proportionate responses, implying that they have or give a sense of scale. This is the reason we have such a penchant for rankings, proportions, and percentages as the scales and weightings are an inherent part of the presentation. “Our number one security risk” clearly has gravitas as does “a highly significant proportion” or “a very high percentage” of something, whereas “much” or “a lot” is vague. As well as focusing attention on the key issues, proportional metrics imply the need for proportionate responses: not only does management need to pay attention to “our top security issue” but it also needs to act smartly, dealing with it before tackling lower-ranking issues.

Once we are able to measure information security consistently and meaningfully, management finally has a handle on security processes and, as such, has the

* Motivation is a major topic in itself, especially when it comes to motivating people about information security. It's a big subject, worthy of another book. For now, take note of how the luminaries in our field— inspirational gurus and thought leaders, such as Bruce Schneier and John Thorp—turn their audiences on to security. Think about the way they position and phrase things, how they put things across, not just literally what they are saying. Motivational techniques can be learnt and practiced. They are just social engineering techniques after all.

Tip: Some metrics seem to take on a life of their own, evolving new meanings or nuances that were never intended and may not be appropriate. If you feel your metrics are starting to drive things the wrong way, it may be necessary to go back to basics and remind the recipients about what is being measured, why it is being measured, what the information means, and what the metric was expected to achieve. Point out gently, if you have to, that people are playing games with the numbers and try to persuade them to work within the system rather than undermining it. If you personally don't have the influence to make an impression, have a quiet word with someone who has the *power*. Ultimately, you may need to retire metrics that simply didn't work out, but that can be tough. The earlier you identify and deal with metrics that are going off course, the less likely you are to suffer a train wreck.

capability to set targets, define hurdles (qualifying criteria and targets), and essentially drive systematic security improvements where necessary. Management can do the following:

- Change the ISMS and the information security controls in response to the numbers
- Periodically recheck the numbers for signs of improvement
- Review, measure, analyze, and act on metametrics in order to improve the measurement system

Consider adapting the message or the presentation style to suit recipients' preferences, worldviews, or personalities.

11.4.1 Periodic versus Event-Driven Reporting

It is generally worthwhile to provide at least a summary of various metrics relevant to managers and other stakeholders periodically or routinely in order to demonstrate that things are ticking along nicely in information security.* In addition, however, consider the value of ad hoc reports triggered by specific events or situations, such as a metric hitting or exceeding a limit, hurdle, or target value (see Section 9.4) or genuinely novel information (insight) emerging from routine data

* Regular reporting periods are normally, by convention, hourly, daily (usually business days only!), weekly, fortnightly (every other week), monthly, bimonthly (every other month), quarterly (every three months), biannually/semiannually (both meaning twice a year), annually (every year), or biennially (once every two years). There is no theoretical reason for using these particular periods, but, in practice, it makes sense to align security reports with other business activities.

analysis. Event-driven reports are, of course, expected to receive extra attention and should be used sparingly, normally only when the information is urgent and a prompt management reaction is anticipated (see Section 9.7).

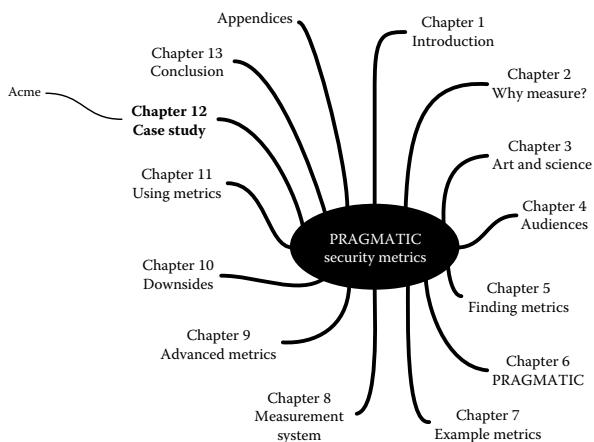
11.5 Summary

This chapter discussed gathering, analyzing, and presenting security metrics in order to have the desired impact on the audience. We described automated and manual data sources, including information that would not normally be considered metrics at all (e.g., the findings of security audits and reviews). After tiptoeing gingerly through a tiny piece of the massive minefield known as statistics, we mentioned creative reporting and presentational techniques and discussed practical issues that crop up when using metrics for real, in real organizations, doing real business. Think of this chapter as an antidote to the rather sterile academic coverage sometimes seen in the security metrics literature. We make no bones about it: we are practitioners, writing for practitioners, and, where appropriate, we're not afraid to cut corners to get the job done.

Free ebooks ==> www.ebook777.com

Chapter 12

Case Study



Example is the best precept.

Aesop

If, despite our best intentions, you find the rest of his book too theoretical, try this chapter for size. Here, we illustrate the specification, selection, and use of security metrics through a case study based on the hypothetical organization outlined below. Throughout this chapter, we refer to {example metrics} drawn from the prototype metrics catalog at Appendix F. Refer back to Chapter 7 for additional information on any that are not immediately obvious.

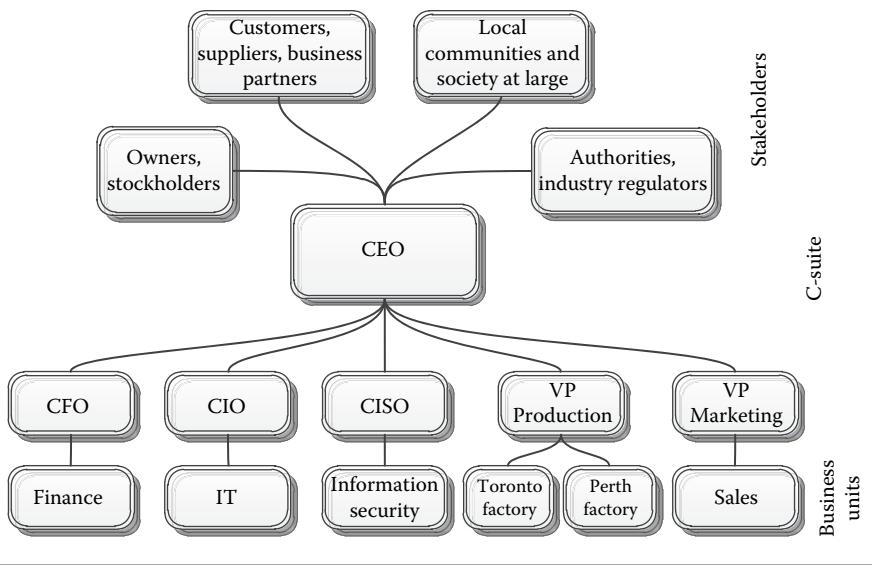


Figure 12.1 Partial organizational chart for Acme Enterprises, Inc.

12.1 The Context: Acme Enterprises, Inc.

For the purposes of this worked example, we envisage Acme Enterprises, Inc., a midsized manufacturing company. The partial organizational structure chart in Figure 12.1 represents some of Acme's executives/senior managers (the C-suite), the business units, departments or functions they manage, plus four external stakeholder groups with varying interests in Acme.*

As mentioned in Section 3.3, a sound approach to specifying and designing metrics is to determine *who* needs to know *what*, *when* in order to effectively discharge their responsibilities. The organizational chart, to a large extent, answers the first question about *who* needs information security metrics, but exploring the security responsibilities in more detail tells us more about the *what*, if not the *when*.

* In reality, information security (and hence information security metrics) would be of wider concern, but these audiences suffice to demonstrate the utility of the PRAGMATIC approach.

12.2 Information Security Metrics for C-Suite

First, let's examine the roles and responsibilities of the senior managers in Acme's C-suite.* Anyone making decisions rationally requires pertinent information, including metrics. The responsibilities noted in the table below imply the nature of the decisions being made and, hence, give us our first real clue about the information and metrics needed.

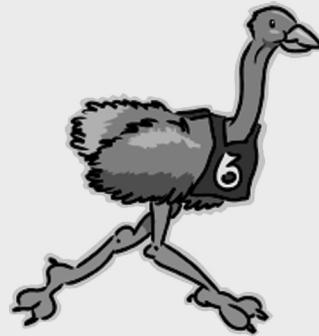
<i>Title</i>	<i>Key Strategic Role</i>	<i>Main Corporate Responsibilities</i>	<i>Information Security Responsibilities</i>	<i>Other Important Responsibilities</i>
CEO	Overall corporate strategic direction	Aligning and optimizing resources, stakeholder liaison, corporate governance	Risk management, asset protection, exploiting information safely, ethics	Overall leadership, coordination and motivation
CFO	Financial and commercial strategies	Profitability: value and revenue generation, cost controls	Financial risk management, financial controls	Regulatory compliance, financial reporting
CIO	Information management strategy	IT and information management, systems and data architecture	IT/data security controls, technical vulnerability management	Technical resilience and IT disaster recovery
CISO	Information security strategy	Information security management (and metrics!)	Information security risk management and controls (all aspects)	Privacy, incident management, continuity planning

* In the interest of actually finishing this book, we are skipping right past the determination of the organization structure and the responsibilities identified in the table. Although it begs fascinating questions, we leave that as an exercise for the reader.

VP marketing	Competitive strategy	Sales and marketing, research and development, distribution and service, competitor analysis	Protection of proprietary knowledge (especially trade secrets), competitive intelligence	Customer relations, advertising and promotions, channels, distribution, pricing
VP production	Manufacturing strategy	Production management, manufacturing	Identifying and protecting critical business processes mostly in the factory	Supply chain and supplier relations, QA, production schedule, efficiency

Let us assume, for the purposes of this case study, that Acme is currently reviewing its business strategy. Let's also assume the draft business strategy is expressed coherently enough through the following paper for us to pick out the key elements, particularly those of relevance to information security.

HIGHLY CONFIDENTIAL



**ACME ENTERPRISES, INC.
DRAFT CORPORATE STRATEGY: 2012–2022**

INTRODUCTION

Once a year, Acme's senior management team meets offsite for a strategic planning meeting to discuss and finalize this draft strategy. The draft is based on the previous year's strategy, incorporating a number of changes, most of

which have been proposed and discussed during the interim quarterly strategic updates.

SCOPE

The strategy applies to the whole of Acme Enterprises, Inc., including the corporate HQ, the widget factories, and the distributed sales and service operations. It is a rolling 10-year strategy.

HISTORICAL PERFORMANCE

During the year since the previous strategic plan was agreed upon, Acme has continued to retrench its core operations as planned, closing the Singapore factory and moving operations to Perth. The extended financial crisis in Europe has led to currency exchange and financing issues beyond those we predicted, delaying a planned move into Eastern Europe.

MARKETS, FINANCES, AND COMMERCIAL OUTLOOK

Difficult trading conditions resulting from global economic problems over the past few years are expected to improve gradually during the next five years, leading to substantial opportunities for growth thereafter, particularly in the Eastern European, North American, and Asian markets. However, increasing competition from the Far East is steadily eroding our margins, particularly given our high fixed manufacturing cost base. Unless we are ready to respond quickly when key markets recover fully from the downturn by 2015, it is likely our lead in the widget market will be lost to our current competitors and new entrants from China in the period 2016–2020; hence, there is a very real need to prepare for changes to our manufacturing operations and, conceivably, our product mix.

SALES AND MARKETING

Despite the present rather difficult commercial situation, the Acme brand remains strong in our home markets, giving us a substantial price premium over imports that are perceived as shoddy and unreliable. In order to maintain our brand, we must continue to invest in marketing and advertising, pushing hard into Eastern Europe, North America, and Asia toward 2015. At the same time, we must take action to protect our trademarks and trade secrets from foreign competition, especially given the high and increasing threats from China, India, and Taiwan. Counterfeit Acme products from Taiwan have already been found as a result of investigating customer complaints when the Singapore operation closed. Our global network of distribution, service, and

support outlets represent a substantial ongoing investment, and we are keen to find ways to maximize their value.

MANUFACTURING AND SUPPLY CHAIN

Acme's factories in Toronto and Perth have served the group well for 30 years but are fast approaching the end of the line. Outsourcing manufacturing to partners or subsidiaries in lower-cost regions will be our prime focus over the next five years, following through on the strategy developed in 2005. Beyond 2017, new relationships with other Western businesses (and possibly mergers/acquisitions in certain areas) will allow us to maintain and extend our manufacturing base still further at low capital cost, mostly through licensing deals exploiting our core manufacturing patents that are due to expire in 2020.

INFORMATION TECHNOLOGY

IT supports and will continue to support Acme in every way possible. However, we are concerned at the implications of changes, such as the introduction of cloud computing, and need more time to evaluate our options in that area.

INFORMATION SECURITY

Protecting Acme's intellectual property (particularly our patent portfolio) remains an important strategic goal; hence, we will be introducing a new set of information security policies in the year ahead, followed by a more comprehensive suite of IT and physical controls in 2013. We anticipate introducing a management system to oversee information security as a whole by 2014 with certification on the horizon for 2015. Looking further ahead, we are very conscious of opportunities to gain more value by exploiting our patents and trademarks through licensing in the period to 2020 and perhaps the move into cloud computing. We intend to work closely with IT and legal to ensure that the appropriate network security, contractual, and compliance controls are ready for when they are needed.

HUMAN RESOURCES

Relocating people from our Singapore operations to Perth proved more difficult than we anticipated; hence, we have been taking on additional employees in Perth, including a substantial number of contractors to tide us over until sufficient permanent employees are trained: this should be complete by the end of 2013. In the period from 2015, we expect to downsize gradually, stabilizing at approximately 50% of our current workforce by 2022 through

a significant loss of manufacturing staff but increases in management and compliance functions as we increasingly turn to outsourcing and partnering.

RESEARCH AND DEVELOPMENT

Our patent portfolio has become an extremely important corporate asset during the past five years, but we have struggled to identify and register as many new patents as we had hoped; hence, we are conscious that many of our existing patents will expire during the next ten years. Therefore, we are planning to increase investment in R&D during the next three years while also exploring cross-licensing options with a number of strategic partners. Cross-licensing is expected to become a substantial source of new business opportunities by 2018, leading to the possibility of joint ventures increasing steadily in number from 2019.

KEY STRATEGIC GOALS

- Consolidate and protect our intellectual property
- Expand our markets in North America and Asia
- Move toward outsourcing and strategic partnerships
- Prepare Acme in advance to exploit new commercial opportunities as they arise

SUBSIDIARY CONSIDERATIONS ON THE STRATEGIC WATCH LIST

- Governance and regulatory burden increasing year by year
- Changing global economy with strong growth of both competition and markets in China and the Far East
- Increasing need to respond more dynamically and flexibly to changes forced upon us

Having considered the structure chart and draft strategy paper,* the next step is to examine Acme's six C-suite managers in more detail, looking into their roles,

* It is a rare strategy that has *no* information security implications. The CISO or information security manager proactively considering the security implications of business strategies might be viewed favorably by the powers that be, and in any event, it is a useful exercise to prepare for eventualities, such as budget cuts if cost reduction is a strong theme or investment opportunities if the strategy talks of growth. It is conceivable that information security considerations might seriously affect the feasibility of certain elements of strategy: finding that out *before* the strategy is agreed upon would be helpful! The search for strategic goals, drivers, or hooks for the information security metrics is, in some ways, a subsidiary consideration. Read the strategy!

business goals, and security objectives in order to select some candidate information security metrics.*

Given senior management's obvious strategic focus, *strategic metrics* are clearly going to be of most interest in the C-suite. Strategic metrics tend to be rather broad in scope with a distinctly forward-looking perspective, like the strategies themselves. Strategic information security metrics support the achievement of Acme's strategic information security objectives, which, in turn, support Acme's business goals, including those stated explicitly in the draft strategy.

12.2.1 Information Security Metrics for the CEO

Acme's chief executive officer provides overall strategic direction and leadership of the entire company, providing broad guiding rules and principles plus a host of other organization-wide big-picture stuff. The CEO is personally accountable to Acme's board of directors and corporate stakeholders for the success or failure of the enterprise as a whole with information security being just one (relatively minor) element of its and his or her performance. The kinds of issues of concern to Acme's CEO include the following:

- Where are Acme's most promising commercial opportunities? Where should Acme be positioned within the competitive landscape? Which markets should Acme be most active in? Which should Acme avoid or pull out of? What is Acme's core business, in fact?
- In what direction should Acme be headed over the years/decades ahead? What opportunities are open to Acme, and what opportunities can Acme create for itself through wise investment?
- What are Acme's greatest strengths? Where does Acme excel, creating unique advantage? In which areas does Acme have significant untapped potential?
- Where are Acme's weak spots? In which respects does Acme substantially trail behind competitors? Where does Acme most need to invest in improvements?
- What are the most significant threats to Acme, both now and in the future?[†] What is Acme's risk appetite? How close to the mark dare Acme run?

* Bear with us here. This chapter starts off slow, real slow, and occasionally meanders away from the Acme example to make a point, but once you've got the gist of it, time will fly past, and before you know it, you'll be skimming the conclusions and pretty soon flying solo. We feel explaining the mechanics of the metrics process will help you handle the realities of dealing with human beings for whom information security is *not* the very center of their life.

[†] And for that matter, given their governance and compliance obligations as the most senior officers of the company, what are the greatest personal threats to Acme's CEO and other senior managers?

- Are Acme's corporate governance and compliance arrangements adequate? Does Acme's executive team work well together, covering all the bases? Is the corporate structure ideal? Are relations with external stakeholders (including owners, regulators, and nonexecutive directors on the board) positive and beneficial?

We move on now to explore eight areas of concern to the CEO in order to identify the types of information needed to support the associated decisions and, hence, determine which information security metrics Acme's CEO might find valuable.

1. Information Security/Business Alignment Metrics for the CEO

Acme's CEO is concerned by the extent to which information security enables, supports, or hinders various business strategies, initiatives, and activities. What information sources and metrics would help the CEO address the strategic alignment issue?

Security governance maturity {metric 6.3} not only tells the CEO how good (or how bad!) Acme's information security arrangements are in relation to generally accepted good security governance practices but also suggests the possibility of the CEO setting improvement targets* and perhaps internal benchmarking (e.g., comparisons and good practice sharing between Acme business units).

Information security ascendency {metric 6.4} is likely to be high given that the CISO is his or her direct report, but what about the other information security people: do they have enough influence? Comparing ascendency ratings on a comparable basis against other corporate functions (such as risk and compliance) might start to get interesting if/when the CEO is thinking about corporate restructures and resourcing levels in preparation for the downsizing mentioned in the HR section of the draft strategy.

Control objectives tied to specific business objectives {metric 6.10} gives the CEO a powerful lever to ensure information security aligns with the business as a whole. It is perfectly reasonable for the CEO to push back on any security investment proposals that do not obviously align with business objectives.

If none of those three metrics is quite right for Acme, there are plenty of other options worth considering, for example, surveying the opinions and perceptions of senior managers regarding the state of strategic alignment or misalignment between the business and information security. Resolving any perceived issues may involve managing the perceptions as much as achieving alignment: for instance, if information security is perceived by certain managers as a barrier or hindrance to the achievement of their strategic goals

* The CISO might expect to find targets of this nature turn up in the personal development plan he or she discusses with the CEO in his or her annual appraisal meeting: it's one way to push corporate goals down through the organization—another use for metrics.

or inappropriate in some way, more detailed information would be needed concerning the nature of the perceived issues. A carefully worded survey, perhaps completed by an independent surveyor on the basis of interviews, group discussions, or the dreaded focus group, will generate useful management information, and the report would typically generate a metric curiously similar to a strategic alignment score. Comparing and contrasting such metrics between functions or business units may identify trouble spots and, conversely, good practices that can be shared around. Significant outliers may need a personal visit by the CEO to determine exactly what the issues are and what needs be done to address them.

2. Information Security Financial/Resourcing Metrics for the CEO

Acme's CEO is concerned with the funding and resourcing of information security risk management, physical security, continuity planning, incident management, compliance, etc., and has a special interest in security improvement initiatives that directly support strategic goals.

Obviously, financial metrics are needed to support financial decisions, but they can be somewhat tricky to determine for information security, risk management, compliance, and assurance activities, which are not entirely financially or profit-motivated, at least not as directly as many other business investments.

Estimated total expenditures on information security related activities {metric 6.15} would give the CEO an overall indication of the cost of information security-related activities across all business units and departments. Comparing the metric between departments or against previous years' figures and projecting future expenditure could prove useful for budgeting and control (e.g., does the R&D function actually increase its security spending as planned to address the security issues relating to the protection of intellectual property?). Categorizing and analyzing security expenses by types of activity (e.g., information security risk management; administration of user IDs, rights, and permissions; physical security; security policies, awareness, and training; business continuity management; incident management; security and privacy compliance) would also be interesting, although the level of detail would probably be more appropriate for the CFO and CISO. However, the metric's mediocre PRAGMATIC score reflects practical difficulties because almost all parts of an organization (not just the CISO's function!) spend on activities that have some bearing on information security (e.g., IT security, physical security, privacy and security compliance, various assurance activities, and information risk management). Security expenditure would therefore need to be defined carefully in order to avoid double counting. The good news is that this issue is common to all corporate/overhead functions and can be dealt with quite effectively through conventional cost-accounting practices, so someone should consult the accountants in finance for assistance to set up appropriate codings in the financial systems.

Benchmarking-type comparisons of security expenditure against other similar organizations might be useful to the CEO *provided* the metric was determined reasonably accurately and certainly on the same basis. Although *security budget as a proportion of IT budget or turnover* {metric 6.28} gets mentioned quite often by the CEO's industry peers at the golf club, the very low PRAGMATIC score suggests this metric is best avoided for actual decision support.*

Information security initiatives conducted as discrete projects within one or more programs will normally be assessed, planned, tracked, and reported using conventional project metrics, including financial metrics. The CEO is no doubt already familiar with *net present value (NPV)* {metric 6.17}, *return on investment (ROI)* {metric 6.18}, and *internal rate of return (IRR)* {metric 6.19} because these are near universal metrics for assessing, tracking, and managing investments. However, he or she may not be so familiar with using them in relation to information security specifically. Many security projects are designed to cut incident costs by improving controls, so metrics comparing the projected incident costs with and without the control improvements would be helpful. At the CEO's level, the detailed business cases and financial performance of individual projects are unlikely to be as relevant as broad aggregate or summary metrics, although the CEO *may* want to dig into the details behind particular figures or projects that catch his or her attention for some reason (typically because there have been problems that lower levels of management have failed to resolve!). Possibly, *value at risk (VAR)* {metric 6.26} or *return on security investment (ROSI)* {metric 6.27} would give a greater focus on security, but to be honest, sound business cases using NPV/ROI/IRR should carry weight regardless of the subject matter and are better accounting metrics. Given the choice, the CEO is more likely to accept familiar over unfamiliar metrics unless there are clear advantages.

Proportionality of expenditure on assurance versus potential impact × likelihood (metric 15.14) is a low-scoring metric largely as a consequence of confusion over the intent resulting from unclear phrasing. The concept of aligning assurance (and security) spending against risk levels is fundamentally sound, so although this specific metric doesn't quite work, a bit of creative thinking and rephrasing might generate similar candidate metrics.[†]

* Don't dismiss it entirely: the metric may yet have value as a deliberate Machiavellian ploy to mislead the competition!

[†] Metrics development is a team sport. If the CEO and other senior managers can be persuaded to spare maybe an hour to participate in an annual metrics workshop, the benefit is not just a set of security metrics that participants find more valuable but a greater mutual appreciation of the issues that really matter and the challenges everyone faces. See Section 8.3, phase 8.

3. Information Security Governance Metrics for the CEO

From a Sarbanes-Oxley (SOX) perspective, the CEO, CFO, and auditors are accountable for governing their respective areas of the business and, as such, are expected to put in place the processes, systems, and structures for management and control. Crucially for them, this includes ensuring vital information flows consistently and reliably from the depths of the organization. Given that the CEO is accountable for Acme's overall performance, he or she must ensure that there are suitable communications paths and mechanisms in place throughout the organization in order to avoid any nasty surprises (e.g., important management information that mysteriously goes missing en route to his or her office or inbox) and serious control failures (e.g., noncompliance with strategies, directives, policies, etc., mandated by management plus laws, regulations, and contractual terms imposed on or accepted by Acme).

Specifically with respect to information security governance, the CEO is concerned that the CISO has the authority to be effective across all the business units and departments.

Candidate metrics here include *security governance maturity* {metric 6.3} and *information security ascendency* {metric 6.4}, both of which have already been proposed for the CEO as metrics supporting strategic alignment, so if selected, they would serve double duty. *Proportion of policy statements unambiguously linked to control objectives* {metric 5.9} is probably too detailed for the CEO unless there are known to be specific issues in this area; in which case, the CEO might want to see that things are progressing under the stewardship of the CISO and information security manager.

4. Information Asset Ownership Metrics for the CEO

Information assets are owned, in the legal sense of property rights, by Acme, by third parties (such as Acme's software suppliers), or by individuals (particularly the subjects of personal data, such as Acme employees and customers). Designating managers within Acme to act as pseudo-owners or custodians for information assets has substantial security benefits, particularly the ability to hold the managers personally accountable for ensuring "their" assets are adequately protected/secured.

Although this is an important control, the CEO only has the time and energy to deal with the ownership and protection of information assets as significant as the general ledger, manufacturing control, the procurement system, and, of course, Acme's extremely valuable and sensitive patents database.

It may be highly PRAGMATIC, but because *number of orphaned information assets without an owner* {metric 7.1} is classified as a management metric, it is more likely to be of interest to Acme's information security manager than the CEO. *Information asset management maturity* {metric 7.2} is the only strategic metric identified in the information asset management examples. Other metrics, such as *integrity of the information asset inventory* {metric 7.5} might,

however, be adapted for the CEO or used to point out specific issues in ad hoc, rather than routine, reporting.*

5. Information Security Risk Metrics for the CEO

The CEO is accountable for the organization's overall management of risks, particularly bet-the-farm risks that could bring the entire organization crashing down. This encompasses *all* types of risk (e.g., financial, commercial, health and safety, IT, personnel, compliance, *and* information security)—hence, a way of assessing relative risk levels would be of interest to the CEO. At the same time, there are inevitably risks associated both with taking business opportunities and with not taking (or missing out on) them, so a metric that somehow indicates both the upside and the downside of risk would be ideal.

One suggestion is a heat map along the lines shown in Figure 12.2.

Strictly speaking, the heat map is not the metric itself but describes the manner in which the actual metric is presented.[†] In this case, somebody has somehow assessed the relative levels of information security risks across the entire organization, assigning the business units and departments into the three categories shown. The actual metric might be *number of high/medium/low risks currently untreated/unresolved* {metric 4.2}, *information security risk scores* {metric 4.6}, or something else. The risk levels are then superimposed on a graphical representation of Acme, where the sizes of the boxes on the map vaguely reflect the relative importance of the corresponding business units and departments.

The map underlay is almost incidental to the heat map as a metric. It is meant to focus attention and stimulate discussion, not to show the precise limits and extents of the issues.[‡] Acme uses a semi-physical view of itself, but it might equally have been some sort of pan-organizational business process map or a hierarchical/stove piped view of the business departments. So long as it has just enough detail to be meaningful, but not so much as to be totally confusing, its aim is met.[§]

* It should be obvious from the text that none of the metrics in our putative metrics catalog (Appendix F) fit the bill perfectly here.

[†] Notice the conspicuous triangle in sales and marketing: the author of the heat map is clearly drawing attention to an issue there, perhaps a significant increase in the level of risk since the previous report or a particular situation that requires urgent attention. In a report, it would link to a note. In a presentation, it would be pointed out and explained by the presenter.

[‡] If you seriously expect the underlying maps used in heat maps to be literal representations, you are sadly deluded: their prime purpose is to give a figurative illustration indicating to management where the main issues lie, not to guide a lost visitor across the factory floor.

[§] By the way, the concept of a map with overlays could easily evolve into a whole series of overlays for different purposes. Measuring control or compliance or something else instead of risk would show how often a department that excels at one thing stinks at another. Re-measuring the risk metric periodically and creating new overlays each time would build up a dynamic picture of the way the risks are changing, almost a cartoon or time-lapse effect. But, remember, metrics are supposed to support decisions, not entertain the children.

334 ■ PRAGMATIC Security Metrics

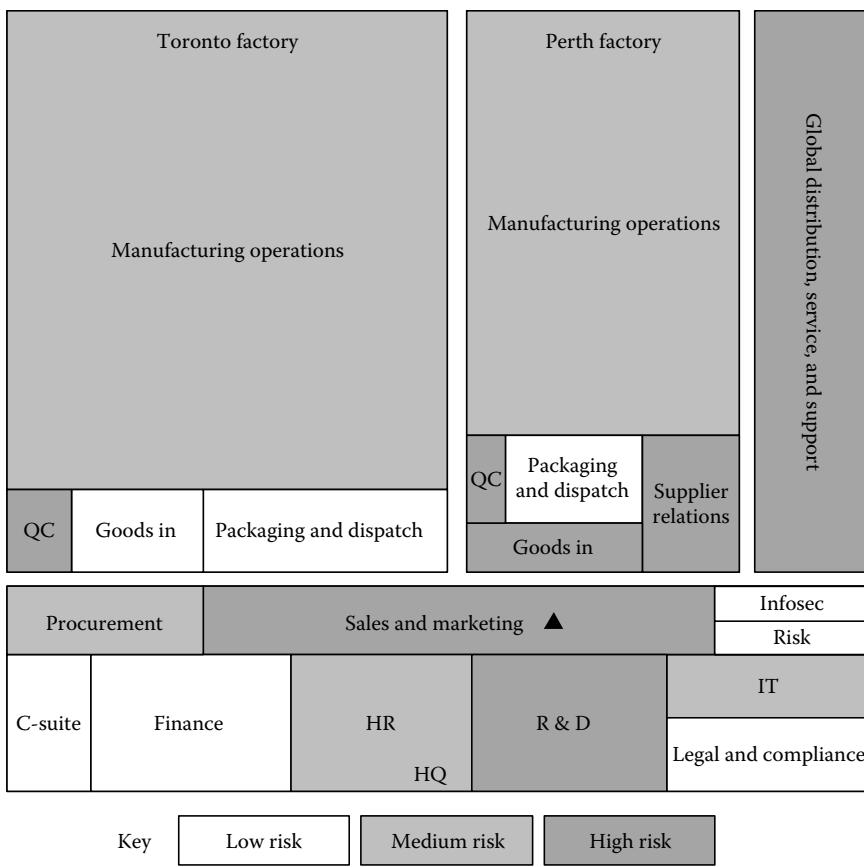


Figure 12.2 Acme information security risk heat map (in glorious monochrome).

Tip: In the hands of a naturally risk-averse information security or risk professional, traffic light reports, heat maps, SWOT/PEST analyses, and other formats are almost exclusively used as a means to highlight the negative aspects of the underlying metrics. However, they can also be used in a far more positive sense, identifying and encouraging the sharing of good practices. Did you spot, for instance, the markedly different risk ratings assigned to the “goods in” functions at the factories? It suggests that goods in, Perth could learn something worthwhile on the security front from their colleagues in Toronto.

An aspect often overlooked by security, risk, and compliance professionals is that the business is seldom best served by eliminating risks: risks should be brought under management control and maintained at an acceptable level, but any further reduction is unnecessary and, in fact, counterproductive because there are inevitably additional costs. Therefore, when presenting and discussing the risk heat map with the CEO and probably other executives, the CISO should resist the urge to imply that a low risk rating is necessarily appropriate. He or she might even go as far as to suggest that security controls should be relaxed a little, cutting security costs in the low risk areas, allowing them to drift gently up toward medium (or optimal) risk.*

Other risk-related metrics candidates from Chapter 7 include *security risk management maturity* {metric 4.1} and *total liability value of untreated or residual risks* {metric 4.7}. We don't have the space to elaborate on the merits of those metrics right now, but it's something you might like to ponder.

6. Information Security Incident Metrics for the CEO

The specific mention of counterfeit Acme goods in the sales and marketing section of the strategy paper constitutes an obvious strategic management concern over the protection of Acme's intellectual property rights (IPR). It could easily be used to justify the need for metrics on IPR-related incidents, such as unauthorized and inappropriate disclosure of trade secrets (e.g., highly confidential proprietary information, such as pre-patent data from R&D) to Acme's competitors.[†] However, the real issue is far broader than IPR because many other types of information-related incidents could equally harm Acme's profitability, reputation, and share value materially. A serious malware infection, hack, software corruption, or outage causing significant data corruption, damage, or loss to vital business information and systems (such as any of the critical systems mentioned earlier) would immediately impact dependent business processes. Such an incident would be very expensive and could be disastrous.[‡] As well as harming relations with the data subjects, a serious privacy breach that becomes public knowledge would be embarrassing both for Acme and for the CEO personally because he or she would no doubt be expected to face up to it in front of a hostile press. Even relatively minor information

* Imagine that! The CISO says we can relax security! The trick is to be selective and cautious about it, but it does make the point that information security is openly supporting the business and not the “no” department.

[†] Acme sometimes *deliberately* discloses its trade secrets to employees, business partners, and patent authorities for good reasons: the concern is specifically with unauthorized and inappropriate disclosure, plus situations in which employees, partners, or authorities betray the trust in them by failing to protect Acme's interests.

[‡] Such incidents would almost certainly be serious enough to merit being brought to the CEO's attention at the time, but incident escalation is a separate issue for the selection of information security metrics for periodic management reports.

security incidents cause accumulating losses that may be significant if they occur in large numbers (death by a thousand cuts).

All things considered, information security incident-related metrics would support the strategic concerns in this area and are probably worth reporting to the CEO.

Four of the incident management example metrics in Section 7.10 are classified as strategic:

- *Information security incident management maturity* {metric 13.1}
- *Cumulative costs of information security incidents to date* {metric 13.5}
- *Number of information security events and incidents, major and minor* {metric 13.6}
- *Nonfinancial impacts of incidents* {metric 13.8}

By far the most PRAGMATIC one is the maturity metric, but in this situation, the other three are closer to what we believe to be of concern to the CEO and the C-suite. This suggests an opportunity to develop a new metric, perhaps combining the best aspects of these three or four. In conjunction with the CEO, we might, for instance, develop a compound metric based on the total impacts of incidents (meaning the obvious financial costs plus a reasonable estimate of the nonfinancial elements), perhaps analyzing these costs by business unit or department and projecting them forward on a reasonable basis to indicate the trends.*

7. Information Security Compliance Metrics for the CEO

We don't know what kind of widgets Acme manufactures, but certainly in some sectors, regulatory sanctions, prosecutions, fines, and other sanctions may constitute huge potential liabilities for the corporation. Violations of SOX, HIPAA (Health Insurance Portability and Accounting Act of 1996), and IPR have resulted in fines in the tens of millions of dollars for other comparable organizations. Dollar figures with so many significant digits inevitably have a galvanizing effect on senior managers.

In theory, Acme should comply fully with its obligations under information security, privacy, governance, and other laws and regulations, plus others such as nondisclosure agreements with business partners, and ethical obligations. Furthermore, certain third parties are supposedly obliged to comply with Acme's information security requirements, such as the privacy clauses specified in its service contracts with IT and telecoms suppliers, and commercial confidentiality clauses in its IPR licensing deals.

In reality, compliance is not the black-and-white issue often implied. Factors such as the potential penalties or sanctions for noncompliance, the likelihood of being caught, the severity of the noncompliance, the costs

* Note the use of both estimation and trends. The proposed metric goes well beyond the realm of factual, historical measurements and would give scientific metriicians sleepless nights, but given the nature of corporate strategy, it seems entirely appropriate to develop such a forward-looking indicator.

involved in achieving and maintaining compliance, and the sheer practicalities of implementing the associated controls consistently across Acme together make compliance a management if not a strategic issue for the CEO.

Information security compliance management maturity {metric 15.1} scores highly and fits the bill as a strategic metric. Best of all, the metric is easy to understand: a compliance maturity score expressed as a simple percentage (in fact, an average of the percentage scores from the rows on the maturity scale in Appendix H) gives an immediately accessible indication of the state of play, and the CEO always has the option to delve into the row scores and the underlying issues for additional assurance.

Status of compliance with externally imposed information security obligations {metric 15.4} and *percentage of security policies supported by adequate compliance activities* {metric 15.9} complement the compliance maturity metric, providing more detail and assurance. If the CEO feels compliance is a vital control issue (so vital that he or she is concerned that the maturity metric might perhaps be sanitized by someone before it reaches his or her desk in order to conceal serious concerns), he or she might use one or other of these metrics to validate the maturity metric.

If Acme is known (as a result of existing metrics in this area) to face some compliance challenges, perhaps benchmarking Acme's compliance practices against other organizations would be another interesting metrics avenue to explore. If Acme is doing better than the comparators from a compliance standpoint, the CEO would probably be pleased to find out. If not, the CEO probably deserves to be told in no uncertain terms where the troubles lie even if the news creates intense displeasure: it is better to find out through internal management information and have the time to respond rationally than to discover such serious issues after the fact through a regulatory enforcement notice!*

Acme's information security compliance liabilities are most likely to include copyright infringement (e.g., software and content that employees download from the Internet without realizing the license implications and, possibly, patent infringements in its manufacturing processes and products) and privacy violations. The take-home message is that metrics relating to potential security liabilities will hopefully give management the opportunity to address them before being sanctioned, and metrics on actual incidents and penalties/costs arising would serve to substantiate the liabilities.

* That comment hints at an issue we haven't covered thus far: it's no fun being the bearer of bad news, but that is exactly what often happens with metrics, especially risk and security metrics. The wise CEO may go purple with rage from time to time, but he or she always, *always*, appreciates the message and warmly rewards the messenger. To do otherwise sets him or her off down the slippery slope known as sanitized reporting that means he or she is the *last* to know things he or she should have known *first*.

8. Information Security Policy Metrics for the CEO

Policies without overt senior management support and mandate tend not to be effective, but neither are supposedly mandatory policies that lack the associated compliance and enforcement activities. Policy compliance is bound to be another area of some concern to the Acme CEO, albeit largely covered by the metrics discussed just above.

A somewhat different issue concerns the coverage and content of the information security policies. If we assume that Acme has its policy approval and compliance activities in hand, the CEO still needs to know that the mandated policies are both appropriate and sufficient. Additional strategic metrics along these lines include *security policy management maturity* {metric 5.2} and *comprehensiveness of security policy coverage* {metric 5.5}. The CISO and CEO could discuss and progress their common interests through these metrics.

9. Other Information Security Metrics (to Be Selected Personally by the CEO)

Our discussion so far in this chapter has mostly centered on finding homes for some of the strategic metrics examples from Chapter 7 and our metrics catalog in Appendix F. If we stopped there, the CEO would be perfectly justified in accusing us of being supply-driven rather than demand-led, which is one of the cardinal sins we mentioned at the end of Chapter 5. To be fair, we have made an effort to identify metrics that align with and support the strategy paper, but the point is that we would really need to collaborate with the CEO to elucidate and address his or her requirements, rather than continually making assumptions based on our own worldview.

Looking back over this section, we have identified far more possible metrics than the CEO could reasonably be expected to use, so we would need to work on reducing our short list in any event.

The final arbiter of what constitutes good security metrics for the CEO is the CEO.

Unless the CEO has actually read this or other metrics books,* we typically end up performing a delicate balancing act—suggesting metrics we favor as a starting point, a way to stimulate the demand without (we hope) constraining or unduly influencing the final choice.

Tip: It's a similar issue to software development, where if the business analysts go to the users with a rough sketch of an architecture, maybe a prototype or a business process storybook of some sort, they stand a much better chance of prompting the creative thought necessary to specify the functional requirements than if they started with a blank sheet and asked "Well, what do you want?"

* Great idea, but distinctly improbable.

12.2.2 Information Security Metrics for the CIO

Let us now consider Acme's chief information officer. In our example scenario, the CIO is responsible for the IT department, which handles all of Acme's IT and telecommunications requirements. He or she reports directly to the CEO.* What are the strategic information security issues on the CIO's plate?

1. Information Management Strategy Metrics for the CIO

Acme's strategy for managing business information is formalized through a master data management process and information catalog, giving an organization-wide view of data architecture and information assets. It is highly interrelated to information security, of course, because confidentiality, integrity, and availability are all critically important considerations for the information being managed and processed.

The metric *control objectives tied to specific business objectives* {metric 6.10} was proposed for Acme's CEO as a measure of the alignment between information security objectives and business goals. If the identical metric will also serve a similar but slightly different purpose for the CIO, we could almost say it comes for free. It should provide useful feedback for the CIO in continuing to develop Acme's information management strategy and subsequently ascertaining its successes and shortcomings.

Number of controls meeting defined control criteria or objectives {metric 6.6}, *percentage of controls tested realistically* {metric 12.2}, and *quality of system security revealed by testing* {metric 12.4} are valuable measures of the frequency, quality, and results of technical controls testing but may be too detailed for the CIO. Perhaps an aggregated or compound metric would be of interest?

Tip: As a practical matter, integrate the design of information security metrics with enterprise data architecture if possible because many metrics will be technical or have technical components, and metrics are a valid category of enterprise information in their own right. Obviously, for IT operations, the majority of metrics are likely to be technical, while at the management level, many metrics will relate to and be derived from IT processes. Furthermore, the depth of analysis and detail typical of enterprise data architectures leads to better security metrics, again both technical and process metrics—a win-win.

* First a quick aside: notice the CIO's distinctly terse and defensive contribution to the draft strategy document. Either he or she was having a particularly bad day when he or she wrote that or else there is an issue there, perhaps a genuine concern about the cloud.

We previously proposed the metric *status of compliance with externally imposed information security obligations* {metric 15.4} for the CEO, and once again, it would be of interest to the CIO (and the CISO for that matter). It is pretty clear that this metric, or something similar, would probably have utility for several executives and would serve as a catalyst for them to address areas of common interest.

2. Technical Security Management Metrics for the CIO

The CIO is charged with overall responsibility for the IT department and, from a security perspective, acts as the senior custodian of Acme's computer data and various business systems that are owned by information asset owners throughout the business. The CIO is the designated information asset owner and, hence, is personally accountable for providing and protecting shared/corporate information assets, such as the Acme data center, corporate networks, general office servers, and the email systems.

To a large extent, the CIO is expected to take the lead on implementation, administration, and oversight of many information security policies and procedures in the IT domain—the technical side of information security. The security requirements are, at times, at odds with his or her overriding responsibility for ensuring acceptable IT performance, but he or she has a productive working relationship with both the CISO and the information security manager who reports to him or her.

For the CIO to properly address the information security aspects of his or her role and decisions, we suggest providing metrics, such as *IT security maturity* {metric 10.1} and *software security maturity* {metric 12.1}. The maturity metric approach has the advantage of providing supporting details if the CIO needs to dig deeper to understand *why* a given security score is less than optimal. It's also a flexible approach in that the scoring norms can be modified to suit Acme's setup and to keep pace with technical developments in the security field.

3. IT/Data Security Control and Vulnerability Management Metrics for the CIO

Technical metrics are often the easiest to acquire, typically resulting in an avalanche of automated data that meet few of the PRAGMATIC criteria other than **Cost** and **Accuracy**. Just because these metrics are easy to obtain doesn't mean they're good, so it would be prudent to consider them with a jaundiced eye and run them through the PRAGMATIC filter. In many cases, the results or outcomes of processes are much more informative than the operational details. For example, the CIO is far more interested in the technical and business impacts of virus infections and the costs of maintaining the antivirus systems than in how many viruses they detected last month.

The number of technical vulnerabilities is another easy to get but not very informative or useful metric for management. Naïve information security managers may be content to provide the scan results from Nessus or ISS as

metrics, but higher management levels are unlikely to be impressed or glean much meaning from the often voluminous reports. At the end of the day, management is concerned with risk, and vulnerability is just one component of the risk equation. Without knowing whether viable threats exist, whether the vulnerabilities are exposed to them, and some idea of the potential business impacts if exploitation occurs, what use are vulnerability metrics to the CIO? Not enough to make any sort of rational management decision.

Given that prevention is the preferred mode of mitigating risks, it could be argued that, rather than focusing solely on vulnerabilities, the CIO should look for opportunities to reduce threats and impacts or, in some cases, avoid the risks entirely. Having a highly effective incident management and business continuity capability or transferring risks through insurance or other contractual arrangements may be the more cost-effective approach to dealing with security risks than trying to address the other components.

That said, vulnerability management is undoubtedly an important part of managing information security risks. From a technical standpoint, vulnerability is the easiest aspect for IT to tackle. Managing security threats and impacts (whether external or internal) is a much tougher problem that generally extends far beyond the remit of the IT department, requiring the CIO to maintain strong relationships with his or her peers in the C-suite.

So what sort of security things should we consider measuring for the CIO? *Number or proportion of security policies addressing viable risks* {metric 5.7} concerns the policy response to threats that are considered credible, particularly those that are known to be currently active having compromised other organizations rather than being purely theoretical (some might say mythical!). As currently stated, the metric presumes security policies are supported by the appropriate controls, which suggests the need for a complementary metric in that area, such as *number of unpatched technical vulnerabilities* {metric 4.5}. The CIO is most concerned about vulnerabilities on Acme's critical information systems supporting its core business processes. If these are compromised by the aforementioned threats, the impacts would cause significant business disruption and reflect badly on IT. Therefore, some analysis of the metric according to the criticality of the systems and the danger levels of the vulnerabilities and threats (e.g., any that are being actively exploited in the field) would provide a more elaborate but useful metric.

Other security metrics for the CIO to consider are as follows:

- *Number of controls meeting defined criteria or objectives* {metric 6.6} and *percentage of controls unambiguously linked to control objectives* {metric 6.5} are of interest, particularly with respect to technical controls that directly support control objectives relating to specific business goals. Clarifying the linkage to things that are important to the business (e.g., controls associated with business-critical IT services and servers) helps the CIO prioritize the security and operational issues on his or her plate.

- *Percentage of security controls that may fail silently* {metric 6.2} is not a very dynamic and exciting measure but acts as a reminder that the correct operation of critical security controls needs to be routinely monitored in some way, not simply implemented and forgotten. Similarly *percentage of technical controls that fail safe* {metric 12.8} does not score well but might be improved in order to emphasize technical controls that are secure by default in critical areas. These are both technical architecture and design issues, best addressed when systems are initially implemented or changed: the CIO is in a position to ensure that system development and change projects take the requirements into account where relevant.
- *Status of compliance with internally mandated (corporate) information security requirements* {metric 15.7} is a way to keep track of the IT department's compliance with the security-related rules defined in applicable policies, procedures, guidelines, etc.

Many of the metrics the CIO would find useful for decision support would probably also be of interest to the CISO. They get together regularly to consider and discuss certain metrics, making joint management decisions that serve both operational requirements as well as security mandates.

12.2.3 Information Security Metrics for the CISO

The chief information security officer has overall responsibility for Acme's information security, including technical/IT security, physical/site security, personnel security (e.g., security awareness and training), and business continuity plus privacy and related aspects (e.g., information asset and risk management, assurance, and compliance). Metrics are necessary to measure and manage each of these domains, although the relationship between metrics and domains is not necessarily one-to-one because there are overlaps, that is, certain metrics have value across multiple responsibilities. Furthermore, the CISO is heavily involved in putting in place the measurement and reporting processes for the security metrics needed by other executives and departments; hence, he or she has oversight of Acme's entire *information security measurement system*. We will explore Acme's measurement system in a few pages, but first, here are a handful of key security metrics that Acme's CISO would find personally indispensable even if there were no system as such.

1. Information Security Governance and Management Metrics for the CISO

For Acme's CISO, governance is largely a matter of influencing the organizational culture positively toward information security, setting the norms of beliefs, behaviors, and expectations. He or she feels corporate culture is primarily determined by the attitudes, communications, and behaviors of senior management and is a more powerful influence than the written rules and regulations. At the same time, he or she accepts that most organizations remain blissfully ignorant of their own corporate cultures—what's more, the

more dysfunctional they are, the less their awareness.* Because culture is a reality the CISO must deal with, it is surely useful to understand the culture and how it might affect security program activities.

Most of the strategic and managerial metrics from Section 7.3 would be relevant to the CISO, but there are so many that it is impracticable to report them all. Overloading management reports with metrics is counterproductive: it confuses the audience and obscures or deflects attention from the issues that really matter under an avalanche of other information. Focus is the answer, so the big question is which key governance and management metrics should the CISO focus on?

Taking the PRAGMATIC method to heart, we might simply start with a short list of metrics with the highest PRAGMATIC scores from Section 7.3. The top four metrics all score above 80%:

- *Quality of security metrics in use* {metric 6.1} is, in fact, a metameetric. That we are using the PRAGMATIC scores here naturally implies the CISO has already selected this metric!
- *Percentage of security controls that may fail silently* {metric 6.2} could be an interesting candidate if, along with the CEO, the CISO accepts the need for assurance on the correct operation of key controls.
- *Security governance maturity* {metric 6.3} and, in fact, all of the maturity metrics in Appendix H are invaluable because they give an overview of all the information security management issues for which the CISO is responsible. The entire family of maturity metrics gets a strong thumbs-up from the CISO.
- *Information security ascendency* {metric 6.4} was a possible metric for the CEO but, arguably, makes more sense for the CISO to apply to the reporting structure within information security management and ideally to compare to ascendency metrics for other corporate functions. It's not something he or she would want to see very often, but it might be useful whenever he or she is reviewing the structure of the department (i.e., an ad hoc report generated on request).

Unfortunately, none of those four metrics perfectly addresses the culture aspect, so the CISO is going to have to look further afield and/or get creative. If he or she has sufficient time and interest to really explore his or her metrics options in detail, he or she might consider other strategic metrics from Section 7.3, the ones that score above 50% anyway, and he or she would probably have a few others in mind, each of which could be PRAGMATIC-rated and added to the metrics catalog.

A quick search through the metrics catalog reveals the promising candidate *tone at the top* {metric 8.5} in the human resources metrics section.

* According to one psychologist, a simple measure of dysfunctionality is the extent to which the internal perception of the organization differs from that of unbiased external observers. Do they have a warped sense of reality?

The metric's PRAGMATIC score is not bad at 58%, so it is certainly one to bear in mind, albeit it might need further development. Looking at the PRAGMATIC numbers shows a low rating for Independence arising from the assumption that the metric would involve some form of self-rating by members of the organization, but the CISO might consider ways to increase the independence through a survey conducted by a dispassionate third party—maybe a consultancy or even the auditors.

On another tack, the addition of new controls often meets with grumbling, grousing, and resistance, and it is fair to say that any control that significantly impacts productivity and profitability will be on the endangered species list if it ever makes it into the wild. A small-scale trial (e.g., within the research and development function at Acme HQ) to pilot metrics on the productivity impacts of security may be a good approach. The metrics arising could then be used to fine-tune the organization's approach, bolster future business cases for security improvement activities, or help persuade recalcitrant managers to swallow the negative effects of security controls for the greater good, that is, to address unacceptable risks.

Often, it is the case that a known significant risk needs to be addressed, but the controls to do so will have an adverse impact on staff productivity. Employing good metrics on the controls' impact combined with information on the potential impacts provides management with the information to make informed decisions about whether to deploy the controls or not. It's important to understand that these sorts of issues aren't security issues; rather they are business decisions that should be based on good information about the risks, the proposed controls, and the tradeoffs.

2. Information Security Risk Metrics for the CISO

Acme's information security program is risk-driven, so the CISO clearly considers risk-related metrics to be vital. *Information security risk scores* {metric 4.6} directly supports the CISO's responsibilities and decisions relating to information security risk management, for example, clarifying Acme's appetite for information security risks, identifying risks that require further treatment, and achieving parity with other forms of risk (such as financial, currency and credit, market, political, and compliance risks). Driving the information security management program on the basis of information security risks also aligns nicely with ISO/IEC 27001 and 27002, taking Acme a step closer to certification in due course.

A heat map-type report showing the risk scores as an overlay across all the areas of ISO/IEC 27002 (e.g., using a mind map similar to Figure 7.1) would show the overall security status of Acme at a glance and would make an excellent visually appealing color graphic for information security management's intranet Web site, perhaps with the ability for viewers to click on any area to reveal the supporting details that led to the headline maturity score.

The drill-down capability makes this concept ideal for the CISO, both to use for his or her own information and to explain Acme's key information security issues to colleagues. As mentioned earlier, the CISO could use the metric to promote the idea of Acme deliberately pushing the boundaries of risk where it is safe to do so.

3. Information Security Strategy Metrics for the CISO

Acme's information security strategy is owned by the CISO but developed in conjunction with the information security manager and other stakeholders to achieve information security risk management objectives defined by senior management. Strategic decisions have to be based on available resources, applicable constraints, and priorities relative to other corporate activities and initiatives. Linking and aligning information security with business strategies is an essential requirement; hence, *control objectives tied to specific business requirements* {metric 6.10} seems worthwhile, both to drive and to demonstrate strategic alignment. It would help the CISO match up information security objectives with business goals and relevant external obligations, such as laws, regulations, contractual commitments, etc.

Standard project management metrics would assist with direction, management, and control of the strategy implementation—things such as actuals against plans for timescales and budgets, critical path analysis, barriers, issues and risks, perhaps even earned value (EV) if the CISO uses an approach similar to Val IT (ITGI 2008b).

4. Information Security Policy Metrics for the CISO

Policies are formal statements of management intent and direction—and possibly expectations—and, as such, must be owned and ratified or mandated by senior management. Notwithstanding the CISO's beliefs about the supremacy of management attitudes over policies, the fact remains that he or she owns almost all of Acme's information security policies, aside from the overarching corporate security policy owned by the CEO, and recognizes their role in terms of laying down Acme's security rules for employees. He or she shares ownership of some policies with other relevant managers (e.g., the CIO is joint owner of the more technical security policies). Along with the supporting standards, procedures, and guidelines, the policies are, in truth, a formal focal point for Acme's information security program. Useful metrics here include *number of security policies, standards, procedures, and metrics with committed owners* {metric 5.1} and *traceability of policies, control objectives, standards, and procedures* {metric 5.3}.

Given his or her overall stewardship role for the security policies, the CISO is mindful of the coverage and quality of Acme's security manual. Are the existing security policies and standards adequate, do they need modification, or are some absent and need to be created? That question begs even bigger questions about the nature and coverage/scope of corporate security standards. Are there significant gaps in security baselines—perhaps entire

classes or categories of information security risk that have not been duly considered or addressed? *Comprehensiveness of security policy coverage* {metric 5.5} seems like it might be a suitable metric, particularly as Acme uses the ISO27k standards and so has a natural basis for comparison.* Two other possibilities might be *number of security policies that are inconsistent with other policies or obligations* {metric 5.15} and *number or proportion of security policies that are clear* {metric 5.13}, but their PRAGMATIC scores relative to other policy metric options suggest they may not be the best options here. Other variants could be the number of policies with unclear audiences or applicability, with no designated owner accountable for compliance, or with inadequate/unclear compliance obligations/liabilities/consequences, but they would need to be scored and compared.

The tongue-in-cheek *thud factor* (*policy verbosity/red tape index, waffle-o-meter*) {metric 5.10} measuring excessive detail in the security policies may not sit well with Acme's rather stiff-lipped C-suite, but it does hint at an area of genuine concern for the CISO, particularly as some of the policy materials that have been written in the dim and distant past are not exactly paragons of clarity. A better metric for Acme might be something more along the lines of *Flesch readability scores* {metric 5.12}, while that mention of the older policies reminds the CISO that the policy review processes need more work; hence, *number of security policies whose review/re-approval is overdue* {metric 5.11} also has merit, not least because the original policies didn't even specify review dates—in other words, measuring this metric will highlight those old crocks that desperately need to be fully updated, totally rewritten, or withdrawn.[†]

5. Information Security Compliance Metrics for the CISO

Once the information security governance stuff is in order (i.e., there is a comprehensive, well-written suite of security policies, standards, and procedures, duly authorized and mandated by management), the spotlight turns to compliance. Acme's compliance with the security policies, etc., needs to be monitored and measured against suitable objectives[‡]...meaning...metrics!

* Acme might equally have adopted some other security framework, such as NIST SP 800-53 FISMA, COBIT, or the Information Security Forum's Standard of Good Practice—or better yet a synthesis of good practices from them all. Regardless of which one or ones Acme uses, the metric could be a mechanism to introduce the others, plus requirements from PCI, SOX, etc.

[†] This is precisely the kind of area in which effective metrics excel. *Systematically* driving improvement is virtually impossible without good metrics.

[‡] Because 100% compliance with all the rules all the time is practically unachievable, it would help enormously if only management would determine which (we hope only a few) policy statements absolutely *must* be fully complied with. Turning this statement on its head, it could be argued that formal security policies should *only* mandate those few specific obligations that are absolutely mandatory, leaving all other discretionary aspects to standards, procedures, guidelines, etc. While that approach has some merit, it is not what commonly happens and would probably create as many new issues as it solves.

Ensuring an adequate level of compliance with various security obligations is a core task for information security management and other compliance-related functions, such as internal audit and legal, as well as being a part of general management.* A key issue for the CISO is to determine whether Acme substantially meets its information security obligations or, more precisely, the obligations for which noncompliance would be totally unacceptable to management.

Proportion of systems checked and fully compliant to applicable (technical) security standards {metric 10.2} and number of deviations identified between configuration repository and actual asset configurations {metric 12.9} address compliance in the area of technical security standards, but the CISO would no doubt appreciate higher-level information regarding security compliance as a whole—perhaps a synthesis of *status of compliance with externally imposed information security obligations {metric 15.4}* and *status of compliance with internally mandated (corporate) information security requirements {metric 15.7}*. Another approach is to measure compliance with, say, password construction rules or patching policies and procedures, treating such narrow areas more as indicators of the overall state of compliance rather than specific measures.

Furthermore, the CISO faces awkward decisions about precisely what to do when noncompliance is discovered. He or she may be expected to decide on behalf of senior management whether to grant exemptions from security policies or other obligations, bearing in mind that lax attitudes toward relatively innocuous discretionary requirements may belie more significant compliance issues with mandatory obligations. Without further thought and discussion, it is not clear which metrics would help with this.

Security reviews and audits are another source of metrics on the general status of compliance with security rules, for example, *correlation between system/configuration logs and authorized change requests {metric 10.4}* or *number of unapproved/unlicensed software installations identified on corporate IT equipment {metric 15.8}*—again, these quite specific measures may be useful indicators of the overall status, and if they are required for other purposes (e.g., security management or operations), the negligible additional cost of reporting to the CISO makes them quite attractive.

6. Business Continuity Metrics for the CISO

Percentage of critical business processes having adequate business continuity arrangements {metric 14.3}, along with *coverage of business impact analyses {metric 14.1}* are obvious candidate metrics given the CISO's business continuity leadership responsibilities. Business continuity is one aspect where the

* By setting policy compliance objectives based on potential impacts, asset classifications, etc., Acme's CISO can determine the need for fail-safe monitoring and robust metrics in its critical areas versus areas that can safely be subject to less frequent or regular inspection with less stringent metrics.

linkages between information security and the business are rock solid. The entire business continuity approach *has* to be business-driven to make any sense. The metrics help the CISO identify and, if necessary, apply additional pressure on any parts of Acme that are evidently not paying sufficient attention to business continuity. Once the basic business impact assessments are completed and suitable continuity arrangements are in place for the critical business processes, these and other metrics in Section 7.11 can be used to keep the ball rolling, ensuring that the whole of Acme has appropriate business continuity arrangements.

12.2.4 Information Security Metrics for the CFO

The chief financial officer is notionally responsible for Acme's financial well-being and profitability, including aspects such as the cost of capital, financial governance and management (including SOX and PCI-DSS compliance), financial risk management, etc. Information security is a relatively minor concern for the CFO, but security clearly does have some impact on the cost base (e.g., expenditure on information security projects and operations, plus the maintenance costs associated with a widely distributed suite of security controls), compliance obligations, risks, and business opportunities as well as protecting "his" financial systems and data from a variety of unacceptable incidents.

Speaking of that, the protection of financial information assets is also of considerable interest to the CEO and the board, making this one aspect worth measuring and reporting at the C-level, although none of the metrics in the catalog (Appendix F) seem ideal—meaning it may be necessary to develop additional metrics or to find creative ways to adapt and reuse those that are already on the list. As an example, *process/system fragility or vulnerability* {metric 4.4} is broadly applicable but could readily be applied more narrowly in the specific context of, say, a review of the resilience of the core financial systems, if not all of Acme's core business systems (in which case a breakdown by system type would be helpful).

The CISO's compliance metrics are of concern to the CFO in several dimensions, that is, the status of compliance with SOX, PCI-DSS, and financial regulations relevant to information protection/security; compliance of the financial systems, processes, and people with security obligations of all types; and the potential liabilities arising from noncompliance, plus the risks relating to security issues. Metrics such as *cumulative costs of information security incidents to date* {metric 13.5} are clearly financial as are those associated with measuring the cost–benefit value of various security improvement projects (NPV, IRR, and so forth).

Business continuity is a significant concern for the core financial systems, which implies the need for adequate resilience, recovery, and perhaps contingency capabilities. The detail behind *mapping critical business processes to disaster recovery and business continuity plans* {metric 14.9} gives the CFO or his or her managers a chance to confirm whether his or her financial processes and, we hope, the

Tip: Involving subject matter experts from finance in the design/selection and implementation of financial information security metrics is a two-way street. Not only is there value in exploiting their specific skills and knowledge to build better metrics (e.g., ensuring that all applicable accounting codes are captured when developing reports from the financial systems on security costs) but they too gain insight into the true meaning and implications of the metrics (e.g., the significant assumptions inevitably made in relation to incident cost metrics). The same principle applies to information security metrics that cross other specialist areas, such as risk, compliance, audit, HR, and IT. This is yet another good reason to treat metrics as a team activity.

associated IT systems are adequately covered in the plans, and metrics arising from continuity exercises and tests will confirm whether the plans are workable. *Business continuity expenditure* {metric 14.10} is another obvious example of a financial information security metric, part of the bigger picture that the CFO and the finance department build up routinely from all the financial information available.

12.2.5 Information Security Metrics for the VP of Production

Acme's vice president of production is in charge of manufacturing and other activities at the factories, which he considers very much *his* home turf (he avoids HQ whenever possible and resents visits from the suits). Thanks largely to the VP's formative years predating the PC, if not the transistor, the factories are traditional rather than modern in style. They have done a great job for many years despite difficult circumstances, which gives the VP tremendous organizational power.

The VP's secretary prints out a selection of important emails for him every morning, which he dutifully red pens well before the morning shift arrives for work. He does now possess a company-issued cellphone, but it is only ever turned on when he travels between the factories, and he never could quite get the hang of text messaging. To be honest, even the power button is awkward, so he doesn't usually bother to switch it off when he flies.

From the CISO's perspective, manufacturing is a bastion of insecurity. The CISO knows that information security threats to the production systems and processes and security vulnerabilities within them should feature highly on the VP of production's watch list, but he also appreciates that his security-centric world creates a distinct bias. In reality, security is just one category of risk, and risk is just one of many concerns in manufacturing. Their focus on output and efficiency is antithetical to certain aspects of information security. Security controls that in any way impede the *real* business of churning out widgets are not

tolerated in the factories, so, for example, shop floor systems don't have user IDs and passwords because users don't actually log in or log off as such (that would be *far* too slow and inconvenient). Shift supervisors use a secret keypad combination to call up some of the more powerful administrative functions on the CNC machine tools, but that particular secret has long since escaped, and nobody is really sure how to change the code. Factory workers who for some reason feel the need to use a networked computer (typically just to answer inane queries from HR about their timesheets) have the option of a lone PC in one corner of the restroom, accessible only during designated rest breaks. The few computers on the shop floor are mostly deep within the bowels of the machine tools or hidden away in grubby cupboards the insides of which the VP hasn't personally seen for decades.

A small army of Acme technicians (the VP's loyal band of grease monkeys) tends diligently to the mechanical machinery, wherever possible leaving those new-fangled computerized tools to maintenance engineers from the companies that originally supplied them. The maintenance engineers scurry about the factory floor much of the time lugging their fancy ruggedized laptops and cellphones, but just so long as things are working fine on the production lines, they might as well be invisible to the VP of production: the only time he ever speaks to any of them is to bark about getting something fixed *pronto!*

Being a realist by nature, the CISO knows his or her chances of implementing worthwhile information security metrics in manufacturing are somewhat remote. He is conscious that the VP will reach retirement age in a year or two. Meanwhile, though he would much rather spend his valuable time on other parts of the business that actually appreciate his input, the information security risks he already knows about at the factories* are enough to give him sleepless nights. He knows something must be done, but the big questions are what and how.

The only real glimmer of light the CISO sees at the end of a long tunnel is the company's strong quality ethos. Product quality is the one area where the VP of production will accept no compromises. He knows all too well that reworking or discarding widgets that fail the quality control checks is wasteful and expensive, and every box of widgets that goes out through dispatch has the VP's smiling face printed on it right alongside his or her personal money-back guarantee, making it a personal hobbyhorse.

The CISO's challenge, then, is to find a way to associate information security positively with product quality in the VP's mind. A metric that helps him achieve that sole aim won't change the world, but it will give him the foot in the factory door that he so desperately needs.

* Let alone those that he is *sure* he would discover if only he could find a way to send his or her best security professionals in there for a good poke around!

Looking through the metrics catalog, the CISO immediately discounts all the technical metrics for obvious reasons. Concepts such as risk and governance are perhaps too esoteric for the VP, although, to be fair, he runs a tight ship in manufacturing without much in the way of red tape.*

After briefly toying with the thought of using *tone at the top* {metric 8.5} or *organizational dysfunction* {metric 8.12} as sticks to bludgeon the VP into submission, the CISO settles on the idea of a metric firmly grounded in the real world—a physical security measure seems most likely to resonate with the VP. *Number of unacceptable physical risks on premises* {metric 9.5} and *number of unsecured access points* {metric 9.4} both have merit, but which one to choose? The latter metric scores higher on the PRAGMATIC scale (75% as opposed to 62%, enough to be considered a genuine difference) and is simpler, whereas the former does introduce the concept of the acceptability or unacceptability of risks. Neither is categorized as a strategic metric, but the only strategic physical metric presently in the catalog, *physical and environmental security maturity* {metric 9.2}, seems way too advanced for this situation.

Rather than wading in with both feet by simply implementing the metric across Acme, in effect imposing it on manufacturing along with all the other functions, the CISO resolves instead to talk about physical security issues with the VP of production.

After sketching out some notes on his or her approach and emailing the VP's secretary to set up an appointment, the CISO phones the VP first thing one morning.[†] A few polite pleasantries exchanged, the CISO casually mentions that he has some nagging concerns about factory security and would like to send one of his or her people to check out the security arrangements. The VP is initially skeptical but when reminded about a recent incident where a pallet of supplies was stolen from the loading dock in Perth, he agrees that perhaps it might be worth a closer look after all. His overriding concern is that the inspection must not interfere with production, which the CISO categorically assures him or her will not be an issue. The conversation is going so well that the CISO decides to be bold and try to bring up the issue of security metrics. He asks the VP whether he would prefer a report from the inspection,[‡] a presentation on the findings, or both. The VP asks for a

* The CISO makes a mental note to ask the VP of production how he does that: perhaps it will give him or her something to say at his or her retirement ceremony.

[†] He knows there's no point in leaving it until much later in the day. *Everyone* knows about the VP's bottle of Glenfiddich filed under "W" for whiskey and his or her tendency to slip quietly away from site around 3 p.m.

[‡] The CISO chooses his or her words carefully. He has in mind a physical security review or a physical penetration test, but "inspection" is what the VP called it without hesitation, so inspection it is.

printed report,* which gives the CISO a brief chance to talk about its format. “I have in mind a brief management report, maybe five to 10 pages maximum, with some relevant photos and notes on the inspector’s findings along with some tables or graphs on the key points and a few improvement points where appropriate. What do you think?”

“That sounds fine,” says the VP, “so long as it is down to me to decide how to take things forward as I see fit. We’re not going to install that CCTV system you proposed last year, no matter what you say!”

The CISO concedes “OK, well, let’s not prejudge the findings at this stage, but I do have a suggestion for you: the factories in Perth and Toronto are more alike than different, so how about we give you the information to compare the two and perhaps transfer good practices between them? I’m thinking about possibly something along the lines of the numbers of physical risks at each factory or maybe just the number of insecure physical access points...” Wanting to bring the conversation to a close, the VP interrupts. “OK, yes, fine, put them both in. Sounds great! Thanks.” And with that, the scene is set. Not only does the CISO have the opportunity he wanted to take a look at the security arrangements in manufacturing, but the VP of production is open to the idea of a report containing comparative security metrics. This small step for the CISO is a giant leap for the VP, almost enough to warrant a celebration.

12.2.6 Information Security Metrics for the VP of Marketing

We trust you have got the idea by now, so, rather than plod on through the systematic selection of information security metrics that might suit Acme’s vice president of marketing, we will instead take a deeper look at the development of just one custom metric for the VP, concerning Acme’s reputation.

First, the background/business context is a crucial to metrics, so let’s consider why reputation is so important to Acme and why it might be something the VP would find worth measuring through information security metrics.

Corporations ranked high in reputation benefit from an average annual stock price increase of 20.1 percent, whereas the shares of the 10 companies ranked lowest in reputation suffered an average annual decline of 1.9 percent.

M. Qoronfleh and R. Vergin

* And the CISO jots a note to himself or herself to send the VP a nicely bound full color management report by courier, rather than the usual email attachment that any other executive would welcome.

Acme has been in business making some of the finest widgets on the market for decades. From the outset, Acme has always taken pride in the quality of its products and (within reason) has always favored quality over price on the basis that customers will not only come back for more of a good product, but they will tell their friends about it. Its longstanding reputation for high-quality products has allowed Acme to establish a sizeable price premium that new entrants to the market cannot match because customers are willing to part with more cash for Acme's fine products than for what they perceive to be shoddy goods from the Far East. Acme's well-established reputation in the marketplace, as well as its profitability, is reflected in the share price, meaning the stock market's valuation of the corporation, which, in turn, affects its cost of capital (e.g., the ability to raise further capital through loans, bonds, and stocks).

The perception of quality and, in fact, the reality of producing well-made products that are both fit for purpose and consistently good has, thus far, saved Acme from succumbing to a rising tide of cut-price imports. However, the VP of marketing is getting more concerned by the month about the possibility of a serious downturn in Acme's fortunes if that quality premium is ever challenged and rejected by the market. A poor product review in an influential media outlet or, worse still, a quality failure or safety issue leading to an embarrassing product recall could be disastrous—even if the root cause turns out to be one of the third-party suppliers that the company is increasingly using.

It takes twenty years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently.

Warren Buffett

Acme's customers' perception of the trustworthiness and reliability of both Acme and Acme's products is one of Acme's most valuable assets, a vital part of the Acme brand and a crucial factor for both customer acquisition and customer retention. At the same time, it is an intangible asset and a fragile one at that. Although reputational damage is acknowledged by the CEO, the VP of marketing, and other executives as one of Acme's top five corporate risks, not a great deal of solid information is presently available to assist in putting a dollar value on reputation risk nor to protect the reputation rationally in relation to the other four top risks and various others below.

Reputation risk is perhaps the most pervasive threat that businesses face, and it's also the most elusive. It can take so many different forms that it's hard to know where to start measuring and mitigating it. It can originate in misperceptions, areas of communication and public opinion which goes far beyond operational risk incidents. Reputation is an amorphous concept. It is intangible. It can change over time (for

better or worse). It is difficult to define. It is difficult to measure. It is difficult, if not impossible, to value (and is assigned no value by our accounting conventions). And yet it is, without question, among the most valuable assets of any company, particularly a global institution... While reputation is intangible, damage to an institution's reputation (and the resulting loss of consumer trust and confidence) can have very tangible consequences—a share price decline, a run on the bank, a spike in policy surrenders, an outflow of assets under management, a drop in new sales, a ratings downgrade, an evaporation of available credit, regulatory investigations, shareholder litigation, etc. Reputation is therefore derived from the way an institution is perceived by its various stakeholders. What these stakeholders see or hear about a company, it reads about it, knows about it, and how they are treated will in turn affect how they will behave toward the organization.

**Deon Binneman; speaker, trainer, and adviser;
Reputation, Stakeholder & Crisis Management**

This is our opportunity to try out the three-step goal–question–metric (GQM) paradigm* to develop metrics for the VP of marketing.

The first step in GQM is to isolate and describe one or more business goals, and here we have the advantage of the draft strategy paper to analyze.[†] From the text in the sales and marketing section (left), these are the key points that occur to us, along with the goals as we perceive them (right):

“Despite the present rather difficult commercial situation, the Acme brand remains strong in our home markets, giving us a substantial price premium over imports that are perceived as shoddy and unreliable.”	Brand strength is clearly important to Acme or, more accurately, the price premium it creates. Maintain Acme’s price premium is goal 1.
“In order to maintain our brand, we must continue to invest in marketing and advertising, pushing hard into Eastern Europe, North America, and Asia toward 2015.”	This is arguably more a plan than a strategy, but it could be phrased as goal 2—to push into new markets

* See Hayden (2010) and Herrmann (2007) for further description and examples of the use of GQM or look up the original materials on GQM in software engineering (and perhaps even further back into the annals).

[†] Acme probably has stacks of other materials describing its business goals, maybe one of those dreadful rah-rah corporate posters laying out Acme’s mission statement, but we hope it’s something more useful—something that says more *on* the lines than *between* them. Concerning just the strategy paper, there are plenty of goals there to launch the GQM process (although we would struggle with the CIO’s piece!). We could always extend the process later to incorporate additional goals while, at the same time, pondering why they were *not* covered by the strategy.

<p>"At the same time, we must take action to protect our trademarks and trade secrets from foreign competition, especially given the high and increasing threats from China, India, and Taiwan. Counterfeit Acme products from Taiwan have already been found as a result of investigating customer complaints when the Singapore operation closed."</p>	<p>This is fascinating in that it identifies a counterfeiting/IPR incident considered serious enough to mention in a strategy paper. But a business goal is lurking in there at the start. In short, goal 3 is to protect Acme's intellectual property (IP)</p>
<p>"Our global network of distribution, service, and support outlets represents a substantial ongoing investment, and we are keen to find ways to maximize their value."</p>	<p>Easy: Maximize value of the distribution, service, and support outlets is goal 4.</p>

We now have four goals to work with. If we were actually using GQM for real, we would probably proceed with all four, but for this chapter, we'll stick with just one—goal 3—because it has the most direct and obvious relevance to information security.*

We *deliberately* phrased the goals very succinctly in order to stimulate lots of questions in the next step.[†] In considering goal 3, here are the initial and subsidiary questions that occurred to us, pretty much as they coursed through our stream of consciousness:

- *What does protect Acme's IP actually mean?* What does it imply? Does it mean the same thing to everyone, or are there different meanings in particular circumstances, different purposes for protecting the IP?
- *What IP is Acme's, in fact?* Do we have an inventory of IP? How accurate, complete, and up to date is it? Who maintains it, and how? Has anyone checked it lately? What is it used for? What else could it be used for? Who determines what does or does not make it into the inventory? What rules are applied? Who determines and applies them?
- *Protect Acme's IP from what?* What is the nature of the risks? What are the threats, the vulnerabilities, the business impacts? Which of those are the most and least concerning? Which are growing, which are reducing in importance? Which ones might we be able to control or mitigate, and which are just *out*

* There's another point here: GQM is not restricted to information security metrics. It could easily be turned into a game to be played right across Acme with a separate round involving rationalizing the goals, questions, and metrics to reduce the inevitable duplication as well as to identify the points of conflict and the gaps. Yet again, the *process* is as valuable as the *output*.

[†] Hayden (2010) emphasizes that goals should be specific, limited, meaningful, attainable, verifiable, contextual, and documented. Mmmm, that rings the metameetric bell! Anyway...

there waiting to pounce? What other risks have we forgotten, and what else might happen that we haven't even considered?

- *Protect which IP?* We kind of *know* that some bits of IP are more valuable than others (the strategy mentioned trademarks, trade secrets, and patents, which we presume are key), but which are the most and least valuable? And why is that? What are the factors that determine the relative value of IP? Are they purely historical, or is there an element of future worth or lifecycle value (in which case, shouldn't we consider the costs as well as the benefits)? Does IP have an absolute value, and if so, how much do we have? What is value in this context: commercial value, worth, book value, cost, projected value, or what? Are we right to presume that only valuable IP is worth protecting, or might there be other considerations as well?
- *How should Acme's IP be protected?* Again, mention of trademarks, trade secrets, and patents suggests legal protection, but what else can, could, should, or must we do? Are we in any way *obliged* to protect Acme's IP (leaving aside the issue of respecting IP belonging to third parties)?
- *Why protect Acme's IP?* It's obvious isn't it? Well no, not necessarily: IP is just one form of corporate asset, an intangible one at that, which makes it hard to define, contain, value, and protect. Is Acme's IP more or less in need of protection than other corporate assets? Is it truly worth protecting, and at what cost?

Once more, if we were using GQM in earnest, we would take each of those questions (the five or six *bold* ones at least) through to the next stage, developing the associated metrics.

Tip: Apart from their intended purpose to develop metrics, those goals and questions could be used in other ways too, getting even more value from the process. Auditors would probably recognize the train of thought because it is very similar to how they develop internal control questionnaires and audit checklists to explore audit topics. Because they do it all the time, experienced auditors are well versed in a wide variety of methods for exactly this kind of creative analysis, some of which may be used instead of, or to complement, GQM—methods such as brainstorming, mind mapping, Ishikawa cause-and-effect diagrams, Post-It group therapy sessions,* and more. Why not get your auditors involved? Most don't bite! Aside from helping you develop better metrics, they will gain more insight into both the metrics and the business processes and activities being measured.

* Writing ideas individually on Post-It notes then sticking them on a whiteboard, discussing them among the group, and clustering related issues together. It's very therapeutic.

For now, we choose to work on developing metrics for the fourth question: “Protect which IP?” The subsidiary questions are helpful here because they naturally suggest parameters that might be worth measuring, and with a bit more creative thought, we can easily think up related or variant metrics:

- *Relative value of different forms of IP*: ranked list of IP values. Average valuations with variance to account for the uncertainties. Total values of IP by business unit, department or function, and by types of IP (perhaps some sort of IP valuation matrix?). IP with no clear owner versus IP with one clear owner versus IP with multiple or disputed ownership.
- *Most-Least important factors determining the value of IP*: distinguish inherent from added value and historical from current projected value. Value can be arrived at in different ways, for example, contribution to revenue might be one; overall value could be considered the difference between book and market valuation; it could be the cost to create it or the loss or impact of losing it, such as when patent protection expires.
- *IP investments*: accounting for the amount invested in developing, maintaining, and exploiting (and protecting!) the IP, in relation to the business value realized plus the amount of locked-in value yet to be released.
- *Comparative IP valuations*: using different valuation methods, assumptions, etc., with some sort of assessment as to the most appropriate, perhaps for different purposes.
-*You get the idea*: none of these metrics is currently in Acme’s metrics catalog, but thanks to this analysis, they might usefully be added, PRAGMATIC scored, and compared with other options.

Figure 12.3 summarizes what we have achieved through GQM.*

Finally,[†] assuming we need to choose between those four metrics, we turn the sausage machine handle one more time for each metric, generating the associated PRAGMATIC scores to help us compare them in a systematic, rational manner.[‡]

* For simplicity, we have shown one-to-one relationships, but they could be many-to-many. Real life is never quite so simple.

[†] Yes, this is step four of three! Call it “GQM Plus” if you like, “PRAGMATIC GQM” maybe.

[‡] It’s OK, we are not going to bore you stiff with that. You have read more than enough about PRAGMATIC scoring to know what it means. We’ll leave it there.

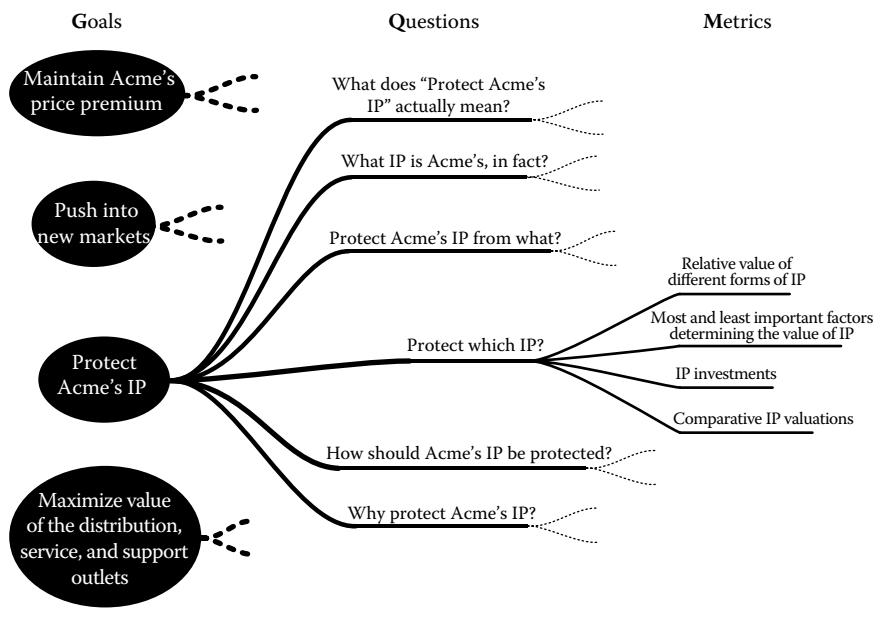


Figure 12.3 GQM example.

12.3 Information Security Metrics for Management and Operations

Whereas to this point we have been banging on about strategic metrics, much the same approaches can be used to generate management and operational metrics for the Acme's middle/junior managers and operations people, respectively.

Given that business managers commonly have limited understanding of information security, the successful CISO or information security manager understands enough of the business to make an informed choice of metrics to supply and the presentation form most likely to result in sound decisions. You could say it is incumbent on the CISO/information security manager to endeavor to understand the decisions a manager makes and then educate him or her on the sorts of things that can be provided to support those decisions. In the end, the decisions made are

Tip: Remember our earlier comments (Section 5.8) about the supply and demand for metrics. Metrics tend to be taken to heart and used more actively and productively if they are chosen—or better still designed—by the people that use them, rather than being imposed upon them. It really pays to get the audience involved in the process.

typically a business judgment call, and, with luck, appropriate metrics will improve that judgment, balancing security concerns with business objectives.

Likewise with operations people—the security analysts, security administrators, systems and network security specialists, and others who need metrics in order to operate and control Acme's systems, machines, and processes they use on a daily basis.

12.4 Information Security Metrics for External Stakeholders

Acme doesn't exist in a vacuum; it is an integral part of the global widget industry alongside its commercial competitors, strategic allies, business partners, and suppliers. It is a major employer for the local areas in which it operates, and its widgets enhance the lives of its customers so much so that they are willing to pay for the privilege of ownership. At the same time, its profits enhance the bank balances of its shareholders/owners, and its taxes reduce the debts of various overstretched governments. These are all stakeholders in the sense that they have an interest in what Acme does, and as such, they are also potential audiences for its metrics, including perhaps its information security metrics.

Some of Acme's external stakeholders have a legal or contractual right to information, examples being the tax authorities, industry regulators, stockholders, banks, and other creditors. Information security information, specifically, does not feature strongly in their demands, although if Acme operated in industry sectors such as financial services, health care, critical infrastructure, utilities, defense, or government agencies/departments, the opposite would be true: those organizations face very specific demands, generally for assurance reasons. As it is, Acme's external auditors can and indeed do demand all sorts of sensitive information about its finances, operations, and controls, and they are taking an increasing interest in information security as Acme drags itself reluctantly into the 21st century. Acme may not be listed on the U.S. stock exchanges, so it escapes the demands of SOX compliance and the dreaded section 404, but other authorities are just as demanding. In Europe, for instance, as this is being written, the European Union's privacy commissioners are upping the ante with every likelihood that, before long, they will insist on rapid, formal disclosure of privacy breaches. In Japan, the authorities already insist, in effect, that many organizations adopt the comprehensive suite of information security controls recommended by ISO/IEC 27002, and ISO27k is creeping gradually into many government departments and large businesses.

PCI-DSS* is another relevant example: as a merchant, Acme accepts credit card payments from customers and, as such, is subject to the explicit information

* Payment card industry–data security standard; see www.pcisecuritystandards.org.

security requirements of PCI-DSS through contracts with its payment processors, the banks, and the credit card companies. PCI-DSS introduces the requirement to accept periodic security audits from accredited auditors and submit compliance reports.

Other stakeholders may not have quite the same legal rights to information about Acme's information security status, but they do have concerns and, arguably, ethical rights in much the same way. Some of Acme's business partners and suppliers are heavily dependent on Acme, so much so that Acme features as a potential risk in their business continuity planning. None have been sufficiently concerned to send in their own teams of inspectors as yet, but if Acme's business situation declines much further under mounting pressure from those much-vaunted cut-throat competitors from the Far East, things may change. Acme's CEO is conscious that some are already making noises, and the more proactive ones are looking to diversify their risks.

A small but conceptually significant step would move Acme from its current position of responding to requests for information to taking the initiative, providing information of its own volition. Acme has already introduced a boilerplate paragraph concerning information security into its annual reports, but if prompted by the CISO, the CEO and VP of marketing might perhaps be persuaded to include one or two headline security metrics, partly for their information content but more importantly to demonstrate to its stakeholders (in not so many words) that it appreciates the legitimacy of their concerns and has matters in hand. Another option might be to start including key information security metrics in its periodic briefings to industry analysts and maybe publish some on the Acme Web site under its quarterly investor updates. Acme doesn't exactly see itself as being in the security industry but quality, reliability, and reputation, all features of the Acme brand, are really not that far from security.

12.5 Acme's Information Security Measurement System

You may have guessed that Acme's senior managers are not exactly ready and willing to design and implement an *information security measurement system* as such, but the CISO is in a position to put some of the foundations in place now with a view to building the system piece-by-piece over the months and years ahead. In time, blockers such as the VP of production will be resolved, but in the short term, the CISO has already made the first moves.

The systems view would take Acme's information security metrics along with its information security management practices to a whole new level, but that is no easy task. It will require the CISO to liaise more closely with other executives and influential managers, discussing and coordinating their requirements for management information (probably developing a discrete metrics thread within Acme's overall data architecture) and together learning from experience. Maturation is the

final phase of the information security measurement system lifecycle described in Section 8.3, but some parts of Acme are barely ready for phase 1!

You will have noticed that Acme's executives sometimes share common interests in certain metrics, but the specific information provided and perhaps the manner of its presentation may need to be tailored to their particular needs. The CIO is undoubtedly more concerned with the security awareness of his or her people than with the awareness level in marketing, for example, and the CISO's purview on awareness extends right across Acme. Some metrics (such as the results of business continuity testing) will be of universal interest and should be made available to all management.

For obvious reasons, management should pay special attention to the quality and reliability of metrics associated with Acme's critical business processes. In terms of information security, the controls around protection and safe exploitation of Acme's IP are a good example: weaknesses in the security arrangements there could be devastating for its future business prospects, and metrics that fail to identify such an impending crisis would be distinctly unhelpful (giving a false sense of security).

As was the case in Chapter 7, the metrics we have suggested in this chapter are merely examples drawn from the prototype metrics catalog (Appendix F). The catalog is far from complete, and the example metrics are not necessarily suited to any particular organization. In practice, management should draw inspiration from a wider variety of sources of candidate metrics as noted in Chapter 5.

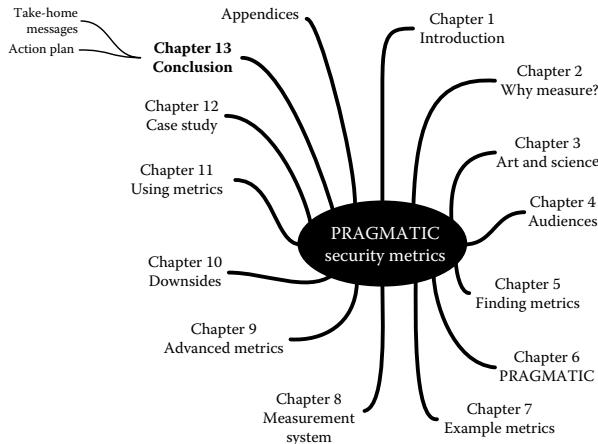
12.6 Summary

Having previously worked through the PRAGMATIC process to rate and select a single metric, discussed the application of a systems approach, and led you on a cook's tour of more than 150 security metrics, this chapter pulls things together through a case study—a worked example describing the selection of key metrics forming the lynchpin of an *information security measurement system* for a hypothetical manufacturing company. Acme may be a figment of our vivid imaginations, but the people, situations, and challenges that Acme faces seem very real to us, being eerily close to people, situations, and challenges we have personally faced at a number of previous employers and clients and plenty more that we have heard about on the grapevine. We have *been there, done that*. And, to be honest, having thought things through in sufficient depth to write this book, we would approach many of the same situations differently a second time around in another life...which is where you come in. We sincerely hope that you can relate to the situations we have described and can benefit from our experience as well as your own.

Free ebooks ==> www.ebook777.com

Chapter 13

Conclusions



To make an end is to make a beginning,
The end is where we start from.

T. S. Eliot

Through this book, we offer what we hope is eminently practical guidance on a very thorny topic, one that is all too often skirted or avoided by information security professionals and business managers, the very people for whom useful information security metrics would be a godsend. We have laid out a rational, step-by-step process for locating, assessing, selecting, and using information security metrics that form the building blocks for a coherent *information security measurement system*.

Fear not, the end is nigh. The time is fast approaching when you will find yourself using our advice in your particular situation, interpreting and adapting it to suit your organization, its security status, the maturity of its ISMS, management's

information and decision support needs, and most of all exploiting opportunities to develop and improve your information security metrics.

13.1 Take-Home Lessons from This Book

We'd like to leave you with some parting thoughts and suggestions on how to take this new knowledge forward, starting with a recap of the main points we have done our level best to bring to your attention.

13.1.1 On Pragmatism and Being PRAGMATIC

Even if you don't entirely agree with the PRAGMATIC criteria and perhaps feel that we have materially mis-scored the example metrics in Chapter 7, surely you will at least acknowledge that the book has stimulated you to think more deeply about security metrics. The same will hold true of your peers, managers, and colleagues. Go ahead; try it. When discussing security metrics, simply mention in passing that you are selecting metrics with the best scores to see how it piques their interest. We encourage you to use our approach to discuss, assess the quality of, compare, and select security metrics. In other words, we have given you the tool and, we hope, the confidence to lift the lid on what has, until now, been a rather nasty can of worms.

By the way, don't feel compelled to design, develop, and implement the perfect security measurement system all by yourself, nor all at once. With such diverse audiences for security metrics, you honestly can't go it alone. Furthermore, because the approach we have described is literally systematic, it can and should be used to drive incremental or evolutionary improvements.* Before you know it, you'll find yourself sitting in or presiding over a periodic management meeting to review the performance of your *information security measurement system* and, as far as we're concerned, that's a job well done!

Notwithstanding previous publications in this field, prior to this book, the selection of information security metrics was largely a black art. For most organizations, it was a hit-or-miss affair. Some took the lead from information security management standards, such as SP800-53 and ISO/IEC 27004, or developed a more systematic approach based on approaches such as COBIT. Some information security professionals simply kept their ears to the ground, picking up metrics

* In the same way, the most valuable feature of an ISO27k ISMS is not a preordained set of security controls designed by some erudite international committee of security experts, but the governance framework for information security with which management can dynamically determine the organization's specific security needs and systematically improve the security controls accordingly. Security metrics are an absolutely essential part of an effective ISMS. The two go very much hand in hand.

tips and suggestions from colleagues, all the while quietly building their own private security metrics catalogs on the basis of their gut feeling and experience. The PRAGMATIC approach doesn't do away with any of these, but it is a game changer. Now, we have a tool to assess and select metrics on a comparable basis and to share our experience with peers in a more meaningful fashion. If you are looking for a metric on physical security for the computer suite, and I tell you I have one that scores very highly on the PRAGMATIC scale, we have a common basis of understanding. At last we can compare information security metrics, pass on good metrics, and generally discuss metrics in a meaningful fashion. We will undoubtedly maintain those private metrics catalogs, but gradually we will converge on common solutions to common problems.

In time (and here we're talking years, possibly decades ahead), information security, risk management, and governance experts will spiral in on a number of good practice security metrics that most organizations find useful and, in fact, use routinely. By consensus, the same core set of information security metrics will start popping up time and again in different organizations, in the press, in training courses, and in textbooks like this one. For us, that will be the sign that information security as a whole has finally matured, reaching the status of a true profession rather than a tradecraft. That's one of our PRAGMATIC metrics.

13.1.2 On Giving You the Confidence and Skills to Have a Go

As with many other planning and analytical processes, we believe the PRAGMATIC process itself to be at least as beneficial as its output. Being a highly accessible and practical process, it brings the hitherto esoteric practice of selecting and implementing information security metrics to a much wider audience. We don't deny that metrics remains an advanced, complex, and difficult area of information security management, not something that a newly minted CISSP or CISM would be expected to tackle unaided, but it is no longer the exclusive preserve of graybeards and overpaid management consultants.

We look forward to seeing PRAGMATIC metrics appear more often on the agenda for management meetings and information security management training courses alike. We welcome feedback from readers who have found this book sufficiently inspirational to take their first baby steps on the road to metrics enlightenment. We're right behind you! But there's one more thing we want you to know: the journey *is* the destination. Developing better metrics is a never-ending mission. In the course of researching, writing, and discussing this book with learned colleagues, our own knowledge has developed, and we know we have more to learn. If nothing else, we hope to have infected you with some of our passion for metrics.

Keep thinking, and keep learning. If your eyes and ears are wide open, you will find inspirational ideas for your information security metrics from a richer variety of sources than you ever thought possible. We are all awash in an ocean of numbers. Instead of clinging desperately to pieces of passing driftwood, hoping to be rescued,

it's time to build first a raft, then a small boat, and eventually one of those sleek, carbon-fiber, race-winning yachts to navigate your way rapidly to the business solutions that good security metrics deliver.

13.1.3 On Improving the Quality of Your Management Information through Metametrics

The nine PRAGMATIC criteria for assessing information security metrics are literally pragmatic: they are founded on our real-world experience in this field, not (except by lucky coincidence) on academic principles. They work for us, producing a much better result than merely considering candidate metrics in an unstructured way. We note with interest, however, that others have, from time to time, suggested their own working definitions of what, to them, constitute good information security metrics, and we openly acknowledge that there may be better metametric criteria than the nine we chose.

In this regard, we wish to point out that metrics and metametrics are forms of information, and, as such, the following is relevant. The exposure draft for COBIT 5 describes three qualities of information with 15 subsidiary considerations that bear a distinct similarity to the PRAGMATIC criteria.

We encourage further academic as well as experiential study in this area in the hope of developing a definitive, generally agreed upon suite of criteria for assessing the quality or business value of metrics.

1. *Intrinsic quality*—the extent to which data values are in conformance with the actual or true values. It includes
 - a. Accuracy—the extent to which information is correct and reliable
 - b. Objectivity—the extent to which information is unbiased, unprejudiced, and impartial
 - c. Believability—the extent to which information is regarded as true and credible
 - d. Reputation—the extent to which information is highly regarded in terms of its source or content
2. *Contextual and representational quality*—the extent to which information is applicable to the task of the information user and is presented in an intelligible and clear manner. It includes
 - a. Relevancy—the extent to which information is applicable and helpful for the task at hand
 - b. Completeness—the extent to which information is not missing and is of sufficient depth and breadth for the task at hand
 - c. Timeliness—the extent to which information is sufficiently up to date for the task at hand

- d. Appropriate amount of information—the extent to which the volume of information is appropriate for the task at hand
 - e. Concise representation—the extent to which information is compactly represented
 - f. Consistent representation—the extent to which information is presented in the same format
 - g. Interpretability—the extent to which information is in appropriate languages, symbols, and units and the definitions are clear
 - h. Understandability—the extent to which information is easily comprehended
 - i. Ease of manipulation—the extent to which information is easy to manipulate and apply to different tasks
3. *Accessibility quality*—the extent to which information is available or obtainable. It includes
 - a. Availability—the extent to which information is available when required or easily and quickly retrievable
 - b. Confidentiality—the extent to which access to information is restricted appropriately to authorized parties

Source: COBIT 5 exposure draft, ISACA (2011)

13.1.4 On Improving Metrics of All Sorts

Go back and take another look at Chapter 5 in the context of other areas of business, other forms of management information. We are convinced that there are many situations—and not just business situations, in fact—in which the design and selection of metrics would benefit from a more systematic and yet practical approach. Could the PRAGMATIC approach be usefully applied there as well? If not, what would need to change? We'll leave you with that parting thought because *we* think we might have really stumbled on something here, but we know we are too close to the wood to see the trees.

13.2 Your Chance to Advance the Profession and the Practice of Metrics

You have already demonstrated remarkable foresight and determination by reading this far, and now comes your big chance to help move things further along.

First of all, we encourage you to chat about metrics with your work colleagues when the opportunities arise. Information security metrics are but one class of metric. The average organization needs many more—for example,

- Risk management metrics, including measures of threats, vulnerabilities, exposures, and impacts
- Health and safety metrics
- Quality metrics concerning fitness for purpose, repeatability of processes, inherent quality, and so forth
- Financial metrics concerning profit and loss, capital and revenue/investment, expense, etc.
- Operations metrics involved in directing, controlling, and improving production activities
- Human resources metrics relating to getting the most out of our people
- Product, market, and customer-related metrics, such as customer churn, innovation, and brand value
- Metrics relating to the organization's overall performance and capability, plus the relative efficiencies and effectiveness of the business units, departments, functions, and teams within it
- Metrics relating to the achievement of a broad range of strategic, tactical, and operational objectives

Speaking with a colleague from, say, a quality assurance function, you may well discover that they too have been struggling to develop worthwhile quality metrics and to report the things that actually matter to management as opposed to those that are easy to measure. Based on the ideas in this book and your own experiences, you should be able to help them find some PRAGMATIC solutions. Conversely, they may already, in fact, have some highly effective metrics, or perhaps they have developed novel approaches to metrics management, analysis, or reporting that would be of value in the information security context. Either way, talking about metrics typically leads to the identification and sharing of good practices within the organization—it's a win-win situation.

Looking a bit further afield, discussing metrics with your professional peers and industry colleagues can be beneficial, including to you personally as patently you have an interest in this field and are receptive to good ideas. Your information security arrangements, including your metrics, *may* (increasingly) be a source of competitive advantage, so you may be reluctant to divulge *everything* to your direct competitors, but on the other hand, we white hats should stick together given that, to a large extent, we face the same issues and common enemies.*

* We have been serially disappointed at the lack of progress on information security metrics catalogs. Projects that have been launched by others appeared to make good progress in the first few months, but then lost their way, most eventually sinking without a trace. We hope we now have the tools we need to compare and contrast our metrics on an even footing. We can discuss and deal sensibly with the duplications, overlaps, and gaps that so often lead to metrics practitioners like us disagreeing, arguing, and eventually falling out when our pet metrics don't quite make the grade on someone else's metrics hit parade.

If information security management is a work in progress, information security metrics are a task barely started. It's a cliché but many hands make light work. If we are to progress as a profession, better minds than ours need to lend a hand at this metrics stuff, so we openly encourage those of you with good ideas to share them with the wider information security community.

Contributors to the discussion forum at SecurityMetametrics.com are helping to drive the profession forward for our mutual benefit. If you have had success with certain security metrics, or conversely, if others didn't work out for you, tell us about it. Raise questions and help answer or clarify those raised by other people. Give us feedback on the book and the PRAGMATIC process. Better information security metrics will raise our credibility and increase our effectiveness. A collective effort through active participation in our SecurityMetametrics forum will go a long way toward achieving those laudable objectives.

13.3 An Action Plan to Take Away

Here are some practical suggestions for things to do after you finish reading this book:

- Go back and run through the case study/worked example (Chapter 12) again, but this time in the context of your own organization. Dig out your organization's business strategy. Look up your organizational chart and find out just how many roles have information security responsibilities if you interpret that as widely as we have. Collect your current crop of information security metrics, and score and rank them using the PRAGMATIC approach. Dig deeper to understand and validate any unexpected results—metrics that end up higher or lower on the list than one might have presumed. For now, keep your analysis up your sleeve.
- Organize a *security metrics workshop* involving information security people; colleagues from related disciplines, such as risk and compliance; a smattering of tame managers; a large coffee pot; and a free morning to brainstorm security objectives and potential security metrics, preferably metrics relating to security objectives that are presently unmeasured.*
- Either in the same meeting or separately, rate and score your security metrics, both existing ones and candidate/proposed additions, using the PRAGMATIC criteria to short list a few candidate metrics that make the grade.

* As is so often the way, the insight and understanding generated by the analytical process are at least as valuable as the output. If there truly are no viable metrics in some areas, management may need to reconsider their objectives!

- Talk the short listed metrics through with management, seeding the idea of an *information security measurement system*; take the opportunity to propose a small pilot study as soon as humanly possible.
- Lather, rinse, repeat.

An important point is to short-circuit the analysis paralysis that often sets in: settle on, implement, and start using metrics that are good enough for now (within reason!) rather than incessantly striving for perfection, knowing that you will be systematically measuring and improving the measurement system (using metameetrics) in due course. It is a bad idea to delay implementing metrics that you already know would be a boon simply to meet some notional task start date on your *information security measurement system* project plan because you are wasting time and missing out on the value you will obtain between now and then. The PRAGMATIC approach is, of course, at the heart of this book. So what are you waiting for?

13.4 Summary

We rounded out the book with some concluding remarks about the PRAGMATIC approach, some upbeat suggestions on how to put it into practice, and an invitation to participate in the ongoing development of information security metrics—because we know our journey to enlightenment is not finished yet. Trust us, there is a lot more left to say and even more to do to push information security kicking and screaming into the 21st century. As regards using metrics and management information in fields such as engineering, finance, HR, operations, and quality, they are all fast approaching the finishing line while we are barely off the starting blocks.

We ended the chapter with an action plan, a prompt to prepare for and organize a metrics workshop to kick off your metrics program and pave the way for an *information security measurement system*.

To sum up, the final mind map (Figure 13.1) gives an overview of the entire book.

We'll leave you now with the information security manager's written response to that internal memo we slipped in at the start of the book. We've given you the tools and techniques to put yourself in his shoes.

Now it's over to you.

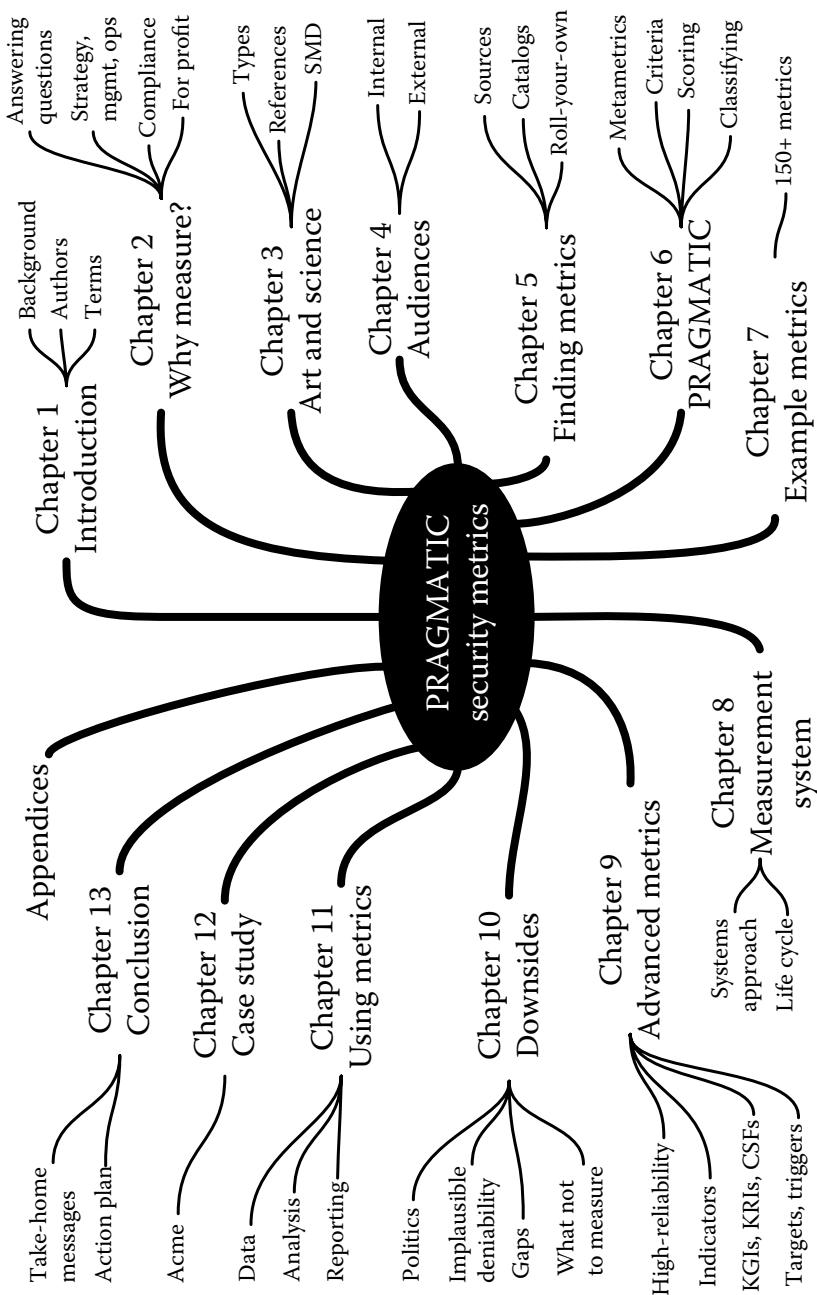


Figure 13.1 Overview mind map.



**ACME ENTERPRISES INC.
ELECTRONIC MAIL SYSTEM**

From: InformationSecurityManager@AcmeEngInc.com
To: ChiefExecutiveOfficer@AcmeEngInc.com
Subject: Information security budget

Dear Fred,

Thank you for the opportunity to explain the basis for the information security budget. As I'm sure you know, we have been quietly developing an information security measurement system comprising a suite of security metrics addressing the very issues you raise, so I hope the following information is exactly what you need.

- a. *Return on investment:* the original business case for the information security management system laid out the projected costs and benefits in order to justify both the initial investment and the ongoing operations. We have been diligently tracking actuals against the plan for the 18 months since we got the green light for the ISMS. I am delighted to report that, although the project consumed all its contingency, the returns have thus far exceeded our expectations (Exhibit 1).

A substantial saving was made by identifying and eliminating approximately 15% of our outdated information security controls without, of course, a corresponding increase in risk. With assistance from finance, we are accounting for the savings on a decreasing basis over five years, and we have instituted a regular controls review process to release further savings.

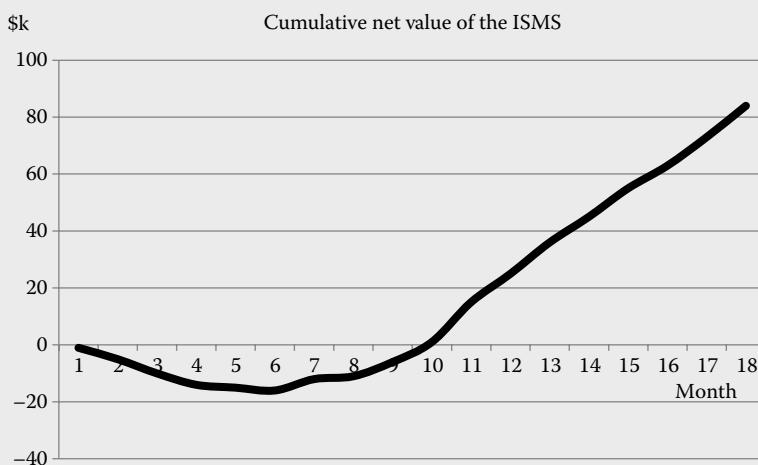


Exhibit 1 Net value of the information security management system.

- b. *Security benchmarking:* although we are not yet confident enough to benchmark Acme against our industry peers, we have been steadily developing our capabilities through internal benchmarking, assessing the main business units against the ISO27k international security standards and comparing them against each other (Exhibit 2).

Thus far, we have identified a number of opportunities and launched three security improvement initiatives covering IT security, access control, and software security at the factories. We are pleased to note the transfer of good practices between the business units in these three areas, and we plan to extend the concept once the initiatives near completion in two to three months.

- c. *Potential security savings:* maintaining information security risks within acceptable limits is the key to keeping information security expenditure in check. Information asset owners (IAOs) throughout the business are accountable for adequately protecting their assets, so they are in the driver's seat making management decisions on the controls they deem

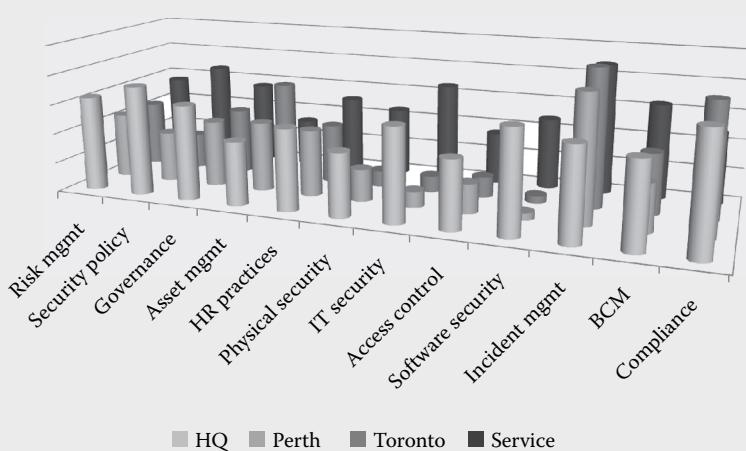


Exhibit 2 Security benchmarking.

necessary albeit under guidance from risk management and information security management. At a broader level, senior managers are responsible for defining risk management and risk assessment methods and the risk appetite. The current top five list shows how information security risks stack up in relation to other risks:

1. Commercial/market risk resulting from Far Eastern competition
2. Theft of Acme intellectual property
3. Compliance failures causing loss of ability to process credit cards
4. Reputational damage, brand devaluation
5. Cloud-computing incident causing loss of IT services

If, as you imply, the information security risks are not at the appropriate level in the list, we would have to work with the IAOs to find ways to reduce the security protecting their assets and accept higher risks. For our own part, we have identified a few areas in which we believe we may be able to improve our efficiency and cost effectiveness and realize substantial savings over five years (Exhibit 3).

As you will see from the data Exhibit 3, we are consciously taking a pragmatic, focused approach to the security metrics we use operationally and for security management, plus those of a more strategic nature that are reported to senior management.



Exhibit 3: Estimated security savings over five years.

Please let me know if you would like to discuss the meaning and/or the way we present the metrics as we would like to incorporate this kind of information into our regular management reports, and we don't want to waste your time with irrelevancies. Given the chance, I would love to help you prepare and perhaps deliver a briefing to the board demonstrating how much we are achieving for the business through our professional, good practice approach to information security.

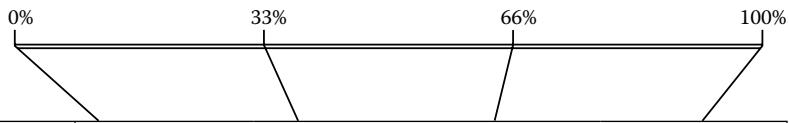
Regards,

John D,

Information Security Manager

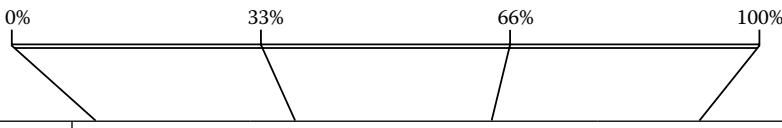
Free ebooks ==> www.ebook777.com

Appendix A: PRAGMATIC Criteria

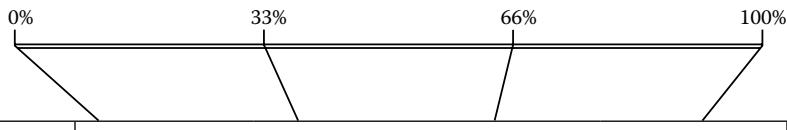


Criterion	<i>Rating Guide</i>			
	0%	33%	66%	100%
PREDICTIVE	The metric is purely historical and backward-looking with no predictive value whatsoever.	Principally historic but gives some vague indication of the future direction, such as weak trends.	Definitely has predictive value, such as strong trends, but some doubt and apparently random variability remains.	Highly predictive, unambiguously indicative of future conditions with very strong cause-and-effect linkages.
RELEVANT	The metric is totally irrelevant to information security.	The metric has marginal relevance to information security with narrow application or some irrelevant aspects.	The metric is quite relevant to information security, but there are a few exceptions or drawbacks.	The metric is absolutely relevant to information security.

378 ■ Appendix A



Criterion	Rating Guide			
	0%	33%	66%	100%
ACTIONABLE	Recipients have absolutely no idea what to do with this metric and so would do nothing at all.	The metric vaguely hints at what needs to be done and might prompt a limited response.	The metric gives a very good steer on what needs to be done and would prompt a suitable response.	The metric is prescriptive, directly actionable, and would definitely cause an appropriate response.
GENUINE	The metric is highly misleading and often totally spurious; sometimes it bears no relation to the truth; it is incredible.	The metric has elements of the truth but lacks credibility: it is dubious or doubtful, being based on unverifiable assertions or assumptions.	The metric is reasonably credible and is supported by verifiable evidence or facts in most important respects.	The metric is entirely based on verified facts and is totally credible: nobody would seriously challenge it.
MEANINGFUL	The metric is completely meaningless and utterly confusing to all its intended recipients.	The metric is somewhat vague and uncertain to its intended recipients; it implies rather than states.	Most of the intended recipients can figure out quite easily what the metric means.	The metric is highly meaningful and crystal clear to its intended recipients: it is patently obvious.
ACCURATE	Random, any resemblance to the facts is purely coincidental.	Vaguely accurate, sometimes wrong, limited precision.	Mostly correct, rarely wrong, reasonably precise.	Highly accurate and precise, always perfectly correct.



Criterion	Rating Guide			
	0%	33%	66%	100%
TIMELY	By the time recipients receive the metric, it is far too late for them to do anything about it.	The metric usually arrives late, limiting the ability to make use of it.	The metric usually arrives in good time but would be of more use if it came even sooner.	Instant/real-time analysis and reporting mean the metric is always bang up to date and immediately usable.
INDEPENDENT	With no independence whatsoever, the metric is highly likely to be manipulated or falsified by those gathering/analyzing the data or reporting it.	There is a distinct possibility that someone might game the system or deliberately mislead recipients by manipulating or falsifying this metric.	There is a slight possibility that the metric might be deliberately manipulated, but at least it could be independently verified to identify this after the fact.	The metric is based on objective data obtained totally independently of the subjects of the measurement.
COST	The metric is prohibitively expensive to measure. It would have negative net value to the organization.	The metric is quite costly but has some net value to the organization.	The metric is quite cheap to measure and has a positive net value to the organization.	The metric is essentially free or has tremendous benefit and, hence, is invaluable to the organization.

Free ebooks ==> www.ebook777.com

Appendix B: Business Model of Information Security (BMIS)

BMIS (Figure B.1) is described by ISACA thus as follows:

1. *Organization design and strategy*: an organization is a network of people, assets, and processes interacting with each other in defined roles and working toward a common goal. An enterprise's strategy specifies its business goals and the objectives to be achieved as well as the values and missions to be pursued. It is the enterprise's formula for success and sets its basic direction. The strategy should adapt to external and internal factors. Resources are the primary material to design the strategy and can be of different types (people, equipment, know-how).

Design defines how the organization implements its strategy. Processes, culture, and architecture are important in determining the design.

2. *People*: this encompasses the human resources and the security issues that surround them. It defines who implements (through design) each part of the strategy. It represents a human collective and must take into account values, behaviors, and biases.

Internally, it is critical for the information security manager to work with the human resources and legal departments to address issues, such as the following:

- Recruitment strategies (access, background checks, interviews, roles, and responsibilities)
- Employment issues (location of office, access to tools and data, training and awareness, movement within the enterprise)
- Termination (reasons for leaving, timing of exit, roles and responsibilities, access to systems, access to other employees)

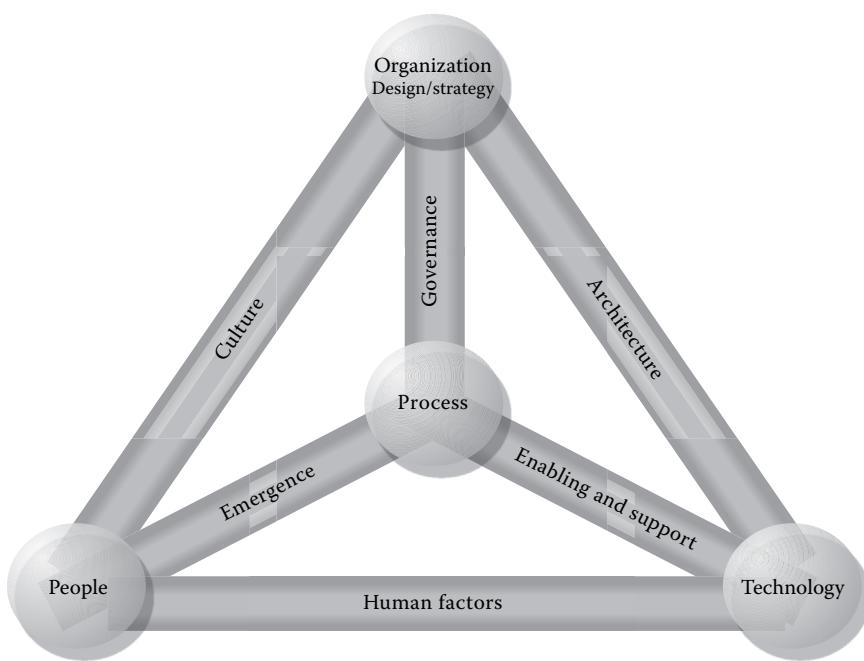


Figure B.1 Business model for information security. (From ISACA, *An Introduction to the Business Model for Information Security*, 2009. With permission.)

Externally, customers, suppliers, media, stakeholders, and others can have a strong influence on the enterprise and need to be considered within the security posture.

3. *Process:* this includes formal and informal mechanisms (large and small, simple and complex) to get things done and provides a vital link to all of the dynamic interconnections. Processes identify, measure, manage, and control risk, availability, integrity, and confidentiality, and they also ensure accountability. They derive from the strategy and implement the operational part of the organizational element.

To be advantageous to the enterprise, processes must do the following:

- Meet business requirements and align with policy
- Consider emergence and be adaptable to changing requirements
- Be well documented and communicated to appropriate human resources
- Be reviewed periodically, once they are in place, to ensure efficiency and effectiveness

4. *Technology:* this is composed of all of the tools, applications, and infrastructure that make processes more efficient. As an evolving element that experiences frequent changes, it has its own dynamic risks. Given the typical

enterprise's dependence on technology, technology constitutes a core part of the enterprise's infrastructure and a critical component in accomplishing its mission.

Technology is often seen by the enterprise's management team as a way to resolve security threats and risks. While technical controls are helpful in mitigating some types of risks, technology should not be viewed as an information security solution.

Technology is greatly impacted by users and by organizational culture. Some individuals still mistrust technology; some have not learned to use it, and others feel it slows them down. Regardless of the reason, information security managers must be aware that many people will try to sidestep technical controls.

Dynamic Interconnections

Dynamic interconnections link the elements together and exert a multidirectional force that pushes and pulls as things change. Actions and behaviors that occur in the dynamic interconnections can force the model out of balance or bring it back to equilibrium. The six dynamic interconnections are:

1. *Governance*: steering the enterprise and demanding strategic leadership. Governing sets limits within which an enterprise operates and is implemented within processes to monitor performance, describe activities, and achieve compliance while also providing adaptability to emergent conditions. Governing incorporates ensuring that objectives are determined and defined, ascertaining that risks are managed appropriately, and verifying that the enterprise's resources are used responsibly.
2. *Culture*: a pattern of behaviors, beliefs, assumptions, attitudes, and ways of doing things. It is emergent and learned, and it creates a sense of comfort. Culture evolves as a type of shared history as a group goes through a set of common experiences. Those similar experiences cause certain responses, which become a set of expected and shared behaviors. These behaviors become unwritten rules, which become norms that are shared by all people who have that common history. It is important to understand the culture of the enterprise because it profoundly influences what information is considered, how it is interpreted, and what will be done with it. Culture may exist on many levels, such as national (legislation/regulation, political, and traditional), organizational (policies, hierarchical style, and expectations), and social (family, etiquette). It is created from both external and internal factors and is influenced by and influences organizational patterns.
3. *Enablement and support*: dynamic interconnection that connects the technology element to the process element. One way to help ensure that people comply with technical security measures, policies, and procedures is to make

processes usable and easy. Transparency can help generate acceptance for security controls by assuring users that security will not inhibit their ability to work effectively. Many of the actions that affect both technology and processes occur in the enablement and support dynamic interconnection. Policies, standards, and guidelines must be designed to support the needs of the business by reducing or eliminating conflicts of interest, remaining flexible to support changing business objectives, and being acceptable and easy for people to follow.

4. *Emergence:* connotes surfacing, developing, growing, and evolving and refers to patterns that arise in the life of the enterprise that appear to have no obvious cause and whose outcomes seem impossible to predict and control. The emergence dynamic interconnection (between people and processes) is a place to introduce possible solutions, such as feedback loops; alignment with process improvement; and consideration of emergent issues in the system design lifecycle, change control, and risk management.
5. *Human factors:* represents the interaction and gap between technology and people and, as such, is critical to an information security program. If people do not understand how to use technology, do not embrace technology, or will not follow pertinent policies, serious security problems can evolve. Internal threats, such as data leakage, data theft, and misuse of data, can occur within this dynamic interconnection. Human factors may arise because of age, experience level, or cultural experiences. Because human factors are critical components in maintaining balance within the model, it is important to train all of the enterprise's human resources on pertinent skills.
6. *Architecture:* a comprehensive and formal encapsulation of the people, processes, policies, and technology that comprise an enterprise's security practices. A robust business information architecture is essential to understanding the need for security and designing the security architecture. It is within the architecture dynamic interconnection that the enterprise can ensure defense in depth. The design describes how the security controls are positioned and how they relate to the overall IT architecture. An enterprise security architecture facilitates security capabilities across lines of businesses in a consistent and cost-effective manner and enables enterprises to be proactive with their security investment decisions.

Appendix C: Capability Maturity Model (CMM)

In *Information Security Governance* (Broby 2009b), Krag described the CMM process as follows.*

Level 1–Initial

At maturity level 1, processes are usually ad hoc, and the organization usually does not provide a stable environment. Success in such organizations depends on the competence and heroics of the people in the organization and not on the use of proven processes. In spite of this ad hoc, chaotic environment, maturity level 1 organizations often produce products and services that work; however, they frequently exceed the budget and schedule of their projects. Maturity level 1 organizations are characterized by a tendency to overcommit, abandon processes in times of crisis, and not be able to repeat their past successes. Level 1 software project success depends on having quality people.

* People interpret and sometimes extend the CMM concept in subtly different ways. For example, in *Information Security Governance: Guidance for Boards of Directors and Executive Management* (ITGI 2005), the IT Governance Institute added a level 0—nonexistent at which “risk assessment for processes and business decisions does not occur. The organisation does not consider the business impacts associated with security vulnerabilities and development project uncertainties. Risk management has not been identified as relevant to acquiring IT solutions and delivering IT services. The organisation does not recognise the need for information security. Responsibilities and accountabilities are not assigned for ensuring security. Measures supporting the management of information security are not implemented. There is no information security reporting and no response process to information security breaches. There is a complete lack of a recognisable system security administration process. There is no understanding of the risks, vulnerabilities and threats to IT operations or the impact of loss of IT services to the business. Service continuity is not considered as needing management attention.”

Level 2–Repeatable

At maturity level 2, software development successes are repeatable. The processes may not repeat for all the projects in the organization. The organization may use basic project management to track cost and schedule. Process discipline helps ensure that existing practices are retained during times of stress. When these practices are in place, projects are performed and managed according to their documented plans.

Project status and the delivery of services are visible to management at defined points (e.g., at major milestones and at the completion of major tasks).

Basic project management processes are established to track cost, schedule, and functionality. The minimum process discipline is in place to repeat earlier successes on projects with similar applications and scope. There is still a significant risk of exceeding cost and time estimates.

Level 3–Defined

The organization's set of standard processes, which is the basis for level 3, is established and improved over time. These standard processes are used to establish consistency across the organization. Projects establish their defined processes by the organization's set of standard processes according to tailoring guidelines. The organization's management establishes process objectives based on the organization's set of standard processes and ensures that these objectives are appropriately addressed.

A critical distinction between level 2 and level 3 is the scope of standards, process descriptions, and procedures. At level 2, the standards, process descriptions, and procedures may be quite different in each specific instance of the process (e.g., on a particular project). At level 3, the standards, process descriptions, and procedures for a project are tailored from the organization's set of standard processes to suit a particular project or organizational unit.

Level 4–Managed

Using precise measurements, management can effectively control the software development effort. In particular, management can identify ways to adjust and adapt the process to particular projects without measurable losses of quality or deviations from specifications. At this level, organizations set quantitative quality goals for both software process and software maintenance. Sub-processes are selected that significantly contribute to overall process performance and are controlled using statistical and other quantitative techniques.

A critical distinction between maturity level 3 and maturity level 4 is the predictability of process performance. At maturity level 4, the performance of processes is controlled using statistical and other quantitative techniques and is quantitatively

predictable (we know how well they are working). At maturity level 3, processes are only qualitatively predictable (we know whether they will work or not).

Level 5—Optimizing

Maturity level 5 focuses on continually improving process performance through both incremental and innovative technological improvements. Quantitative process-improvement objectives for the organization are established, continually revised to reflect changing business objectives, and used as criteria in managing process improvement. The effects of deployed process improvements are measured and evaluated against the quantitative process-improvement objectives. Both the defined processes and the organization's set of standard processes are targets of measurable improvement activities.

Process improvements to address common causes of process variation and measurably improve the organization's processes are identified, evaluated, and deployed. Optimizing processes that are nimble, adaptable, and innovative depends on the participation of an empowered workforce aligned with the business values and objectives of the organization. The organization's ability to respond rapidly to changes and opportunities is enhanced by finding ways to accelerate and share learning.

A critical distinction between maturity level 4 and maturity level 5 is the type of process variation addressed. At maturity level 4, processes are concerned with addressing the special causes of process variation and providing statistical predictability of the results. Although processes may produce predictable results, the results may be insufficient to achieve the established objectives. At maturity level 5, processes are concerned with addressing common causes of process variation and changing the process (i.e., shifting the mean of the process performance) to improve process performance (while maintaining statistical probability) to achieve the established quantitative process-improvement objectives.

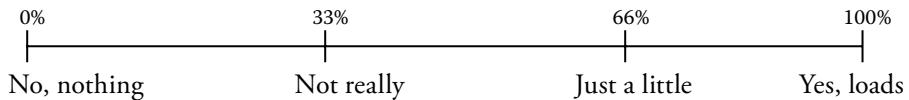
Free ebooks ==> www.ebook777.com

Appendix D: Example Opinion Survey Form

Security Awareness Survey on Malware

We are keen to find out how well the information security awareness program is working. The program recently covered malware, and we'd like to know whether it made an impression on you. Simply consider the questions and mark the appropriate points on the percentage scales (between the markers if you like).

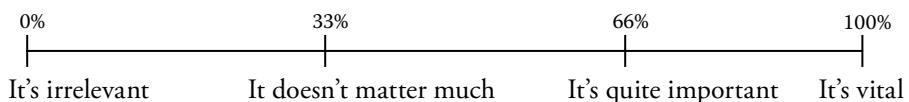
Did you know much about malware *before* it was covered by the security awareness program?



How well do you feel you understand malware *now*?



In your opinion, how important an issue is malware to the organization?



Your thoughts on malware and information security in general will help us improve the awareness program. If you have any feedback suggestions or ideas, please write them in the spaces above, on the other side of this sheet, or contact the information security manager directly. Thank you for your input.

Free ebooks ==> www.ebook777.com

Appendix E: SABSA Security Attributes Table

<i>Business Attribute</i>	<i>Attribute Explanation</i>	<i>Metric Type</i>	<i>Suggested Measurement Approach</i>
<i>User Attributes</i>	<i>These attributes are related to the user's experience of interacting with the business system.</i>		
Accessible	Information to which the user is entitled to gain access should be easily found and accessed by that user.	Soft	Search tree depth necessary to find the info.
Accurate	The information provided to users should be accurate within a range that has been pre-agreed upon as being applicable to the service being delivered.	Hard	Acceptance testing on key data to demonstrate compliance with design rules.
Anonymous	For certain specialized types of service, the anonymity of the user should be protected.	Hard	Rigorous proof of system functionality.
		Soft	Red team review.*
Consistent	The way in which login, navigation, and target services are presented to the user should be consistent across different times, locations, and channels of access.	Hard	Conformance with design style guides.
		Soft	Red team review.

* A red team review is an objective appraisal by an independent team of experts who have been briefed to think either like the user or like an opponent or attacker, whichever is appropriate to the objectives of the review.

392 ■ Appendix E

<i>Business Attribute</i>	<i>Attribute Explanation</i>	<i>Metric Type</i>	<i>Suggested Measurement Approach</i>
Current	Information provided to users should be current and kept up to date within a range that has been pre-agreed upon as being applicable for the service being delivered.	Hard	Refresh rates at the data source and replication of refreshed data to the destination.
Duty-segregated	For certain sensitive tasks, the duties should be segregated, so no user has access to both aspects of the task.	Hard	Functional testing.
Educated and aware	The user community should be educated and trained so that they can embrace the security culture and so as to have sufficient user awareness of security issues that behavior of users is compliant with security policies.	Soft	Competence surveys.
Informed	The user should be kept fully informed about services, operating procedures, operational schedules, planned outages, and so on.	Soft	Focus groups or satisfaction surveys.
Motivated	The interaction with the system should add positive motivation to the user to complete the business tasks in hand.	Soft	Focus groups or satisfaction surveys.
Protected	The user's information and access privileges should be protected against abuse by other users or by intruders.	Soft	Penetration test (could be regarded as "hard" but only if a penetration is achieved; failure to penetrate does not mean that penetration is impossible).

<i>Business Attribute</i>	<i>Attribute Explanation</i>	<i>Metric Type</i>	<i>Suggested Measurement Approach</i>
Reliable	The services provided to the user should be delivered at a reliable level of quality.	Soft	A definition of “quality” is needed against which to compare.
Responsive	The users obtain a response within a satisfactory period of time that meets their expectations.	Hard	Response time
Supported	When a user has problems or difficulties in using the system or its services, there should be a means by which the user can receive advice and support, so the problems can be resolved to the satisfaction of the user.	Soft	Focus groups or satisfaction surveys, independent audit and review against security architecture capability maturity model.*
Timely	Information is delivered or made accessible to the user at the appropriate time or within the appropriate time period.	Hard	Refresh rates at the data source and replication of refreshed data to the destination
Transparent	Providing full visibility to the user of the logical process but hiding the physical structure of the system (as a URL hides the actual physical locations of Web servers)	Soft	Focus groups or satisfaction surveys, independent audit and review against security architecture capability maturity model.
Usable	The system should provide easy-to-use interfaces that can be navigated intuitively by a user of average intelligence and training level (for the given system). The user’s experience of these interactions should be at best interesting and at worst neutral.	Soft	Numbers of clicks or keystrokes required. Conformance with industry standards—for example, color palettes—feedback from focus groups.

* The type of architectural capability maturity model referred to is based upon the ideas of capability maturity models.

394 ■ Appendix E

<i>Business Attribute</i>	<i>Attribute Explanation</i>	<i>Metric Type</i>	<i>Suggested Measurement Approach</i>
<i>Management Attributes</i>	<i>These attributes are related to the ease and effectiveness with which the business system and its services can be managed.</i>		
Automated	Wherever possible (and depending upon cost/benefit factors), the management and operation of the system should be automated.	Soft	Independent design review.
Change-managed	Changes to the system should be properly managed so that the impact of every change is evaluated and the changes are approved in advance of being implemented.	Soft	Documented change management system with change management history evaluated by independent audit.
Controlled	The system should at all times remain in the control of its managers. This means the management will observe the operation and behavior of the system, will make decisions about how to control it based on these observations, and will implement actions to exert that control.	Soft	Independent audit and review against security architecture capability maturity model.
Cost-effective	The design, acquisition, implementation, and operation of the system should be achieved at a cost that the business finds acceptable when judged against the benefits derived.	Hard	Individual budgets for the phases of development and for ongoing operation, maintenance, and support.
Efficient	The system should deliver the target services with optimum efficiency, avoiding wastage of resources.	Hard	A target efficiency ratio based on (INPUT VALUE)/(OUTPUT VALUE)

<i>Business Attribute</i>	<i>Attribute Explanation</i>	<i>Metric Type</i>	<i>Suggested Measurement Approach</i>
Maintainable	The system should be capable of being maintained in a state of good repair and effective, efficient operation. The actions required to achieve this should be feasible within the normal operational conditions of the system.	Soft	Documented execution of a preventive maintenance schedule for both hardware and software, correlated against targets for continuity of service (such as MTBF*).
Measured	The performance of the system against a variety of desirable performance targets should be measured so as to provide feedback information to support the management and control process.	Hard	Documented tracking and reporting of a portfolio of conventional system performance parameters, together with other attributes from this list.
Supportable	The system should be capable of being supported in terms of both the users and the operations staff, so all types of problems and operational difficulties can be resolved.	Hard	Fault-tracking system providing measurements of MTBF, MTTR, [†] and maximum time to repair with targets for each parameter.
<i>Operational Attributes</i>	<i>These attributes describe the ease and effectiveness with which the business system and its services can be operated.</i>		
Available	The information and services provided by the system should be available according to the requirements specified in the SLA.	Hard	As specified in the SLA.
Continuous	The system should offer continuous service. The exact definition of this phrase will always be subject to a service level agreement (SLA).	Hard	Percentage of up-time correlated versus scheduled or unscheduled downtime or MTBF or MTTR.

* MTBF means mean time between failures.

† MTTR means mean time to repair.

396 ■ Appendix E

<i>Business Attribute</i>	<i>Attribute Explanation</i>	<i>Metric Type</i>	<i>Suggested Measurement Approach</i>
Detectable	Important events must be detected and reported.	Hard	Functional testing.
Error-free	The system should operate without producing errors.	Hard	Percentage or absolute error rates (per transaction, per batch, per time period, etc.).
Interoperable	The system should interoperate with other similar systems, both immediately and in the future, as intersystem communication increasingly becomes a requirement.	Hard	Specific interoperability requirements.
Monitored	The operational performance of the system should be continuously monitored to ensure other attribute specifications are being met. Any deviations from acceptable limits should be notified to the systems management function.	Soft	Independent audit and review against security architecture capability maturity model.
Productive	The system and its services should operate so as to sustain and enhance productivity of the users with regard to the business processes in which they are engaged.	Hard	User output targets related to specific business activities.
Recoverable	The system should be able to be recovered to full operational status after a breakdown or disaster in accordance with the SLA.	Hard	As specified in the SLA.

Business Attribute	Attribute Explanation	Metric Type	Suggested Measurement Approach
Risk Management Attributes	<i>This group of attributes describes the business requirements for mitigating operational risk. This group most closely relates to the security requirements for protecting the business.</i>		
Access-controlled	Access to information and functions within the system should be controlled in accordance with the authorized privileges of the party requesting the access. Unauthorized access should be prevented.	Hard	Reporting of all unauthorized access attempts, including number of incidents per period, severity, and result (did the access attempt succeed?).
Accountable	All parties having authorized access to the system should be held accountable for their actions.	Soft	Independent audit and review against security architecture capability maturity model with respect to the ability to hold accountable all authorized parties.
Assurable	There should be a means to provide assurance that the system is operating as expected and that all of the various controls are correctly implemented and operated.	Hard	Documented standards exist against which to audit.
		Soft	Independent audit and review against security architecture capability maturity model.
Assuring honesty	Protecting employees against false accusations of dishonesty or malpractice.	Soft	Independent audit and review against security architecture capability maturity model with respect to the ability to prevent false accusations that are difficult to repudiate.

398 ■ Appendix E

<i>Business Attribute</i>	<i>Attribute Explanation</i>	<i>Metric Type</i>	<i>Suggested Measurement Approach</i>
Auditable	The actions of all parties having authorized access to the system and the complete chain of events and outcomes resulting from these actions should be recorded, so this history can be reviewed. The audit records should provide an appropriate level of detail in accordance with business needs.	Soft	Independent audit and review against security architecture capability maturity model.
	The actual configuration of the system should also be capable of being audited so as to compare it with a target configuration that represents the implementation of the security policy that governs the system.	Hard	Documented target configuration exists under change control with a capability to check the current configuration against this target.
		Soft	Independent audit and review against security architecture capability maturity model.
Authenticated	Every party claiming a unique identity (i.e., a claimant) should be subject to a procedure that verifies that the party is indeed the authentic owner of the claimed identity.	Soft	Independent audit and review against security architecture capability maturity model with respect to the ability to successfully authenticate every claim of identity.
Authorized	The system should allow only those actions that have been explicitly authorized.	Hard	Reporting of all unauthorized actions, including number of incidents per period, severity, and result (did the action succeed?)

<i>Business Attribute</i>	<i>Attribute Explanation</i>	<i>Metric Type</i>	<i>Suggested Measurement Approach</i>
		Soft	Independent audit and review against security architecture capability maturity model with respect to the ability to detect unauthorized actions.
Capturing new risks	New risks emerge over time. The system management and operational environment should provide a means to identify and assess new risks (new threats, new impacts, or new vulnerabilities).	Hard	Percentage of vendor-published patches and upgrades actually installed.
		Soft	Independent audit and review against security architecture capability maturity model of a documented risk assessment process and a risk assessment history.
Confidential	The confidentiality of (corporate) information should be protected in accordance with security policy. Unauthorized disclosure should be prevented.	Hard	Reporting of all disclosure incidents, including number of incidents per period, severity, and type of disclosure.
Crime-free	Cyber-crime of all types should be prevented.	Hard	Reporting of all incidents of crime, including number of incidents per period, severity, and type of crime.

400 ■ Appendix E

<i>Business Attribute</i>	<i>Attribute Explanation</i>	<i>Metric Type</i>	<i>Suggested Measurement Approach</i>
Flexibly secure	Security can be provided at various levels, according to business need. The system should provide the means to secure information according to these needs and may need to offer different levels of security for different types of information (according to security classification).	Soft	Independent audit and review against security architecture capability maturity model.
Identified	Each entity that will be granted access to system resources and each object that is itself a system resource should be uniquely identified (named) such that there can never be confusion as to which entity or object is being referenced.	Hard	Proof of uniqueness of naming schemes.
Independently secure	The security of the system should not rely upon the security of any other system that is not within the direct span of control of this system.	Soft	Independent audit and review against security architecture capability maturity model of technical security architecture at conceptual, logical, and physical layers.
In our sole possession	Information that has value to the business should be in the possession of the business, stored and protected by the system against loss (as in no longer being available) or theft (as in being disclosed to an unauthorized party). This will include information that is regarded as intellectual property.	Soft	Independent audit and review against security architecture capability maturity model.

<i>Business Attribute</i>	<i>Attribute Explanation</i>	<i>Metric Type</i>	<i>Suggested Measurement Approach</i>
Integrity-assured	The integrity of information should be protected to provide assurance that it has not suffered unauthorized modification, duplication, or deletion.	Hard	Reporting of all incidents of compromise, including number of incidents per period, severity, and type of compromise.
		Soft	Independent audit and review against security architecture capability maturity model with respect to the ability to detect integrity compromise incidents.
Non-repudiable	When one party uses the system to send a message to another party, it should <i>not</i> be possible for the first party to falsely deny having sent the message or to falsely deny its contents.	Hard	Reporting of all incidents of unresolved repudiations, including number of incidents per period, severity, and type of repudiation.
		Soft	Independent audit and review against security architecture capability maturity model with respect to the ability to prevent repudiations that cannot be easily resolved.

402 ■ Appendix E

<i>Business Attribute</i>	<i>Attribute Explanation</i>	<i>Metric Type</i>	<i>Suggested Measurement Approach</i>
Owned	There should be an entity designated as the owner of every system. This owner is the policy maker for all aspects of risk management with respect to the system and exerts the ultimate authority for controlling the system.	Soft	Independent audit and review against security architecture capability maturity model of the ownership arrangements and of the management processes by which owners should fulfill their responsibilities and of their diligence in so doing.
Private	The privacy of (personal) information should be protected in accordance with relevant privacy or data protection legislation and so as to meet the reasonable expectation of citizens for privacy. Unauthorized disclosure should be prevented.	Hard	Reporting of all disclosure incidents, including number of incidents per period, severity, and type of disclosure.
Trustworthy	The system should be able to be trusted to behave in the ways specified in its functional specification and should protect against a wide range of potential abuses.	Soft	Focus groups or satisfaction surveys researching around the question "Do you trust the service?"
<i>Legal and Regulatory Attributes</i>	<i>This group of attributes describes the business requirements for mitigating operational risks that have a specific legal or regulatory connection.</i>		
Admissible	The system should provide forensic records (audit trails and so on) that will be deemed admissible in a court of law should that evidence ever need to be presented in support of a criminal prosecution or a civil litigation.	Soft	Independent audit and review against security architecture capability maturity model by computer forensics expert.

<i>Business Attribute</i>	<i>Attribute Explanation</i>	<i>Metric Type</i>	<i>Suggested Measurement Approach</i>
Compliant	The system should comply with all applicable regulations, laws, contracts, policies, and mandatory standards, both internal and external.	Soft	Independent compliance audit with respect to the inventories of regulations, laws, policies, etc.
Enforceable	The system should be designed, implemented, and operated such that all applicable contracts, policies, regulations, and laws can be enforced by the system.	Soft	Independent review of (1) inventory of contracts, policies, regulations, and laws for completeness and (2) enforceability of contracts, policies, laws, and regulations on the inventory.
Insurable	The system should be risk-managed to enable an insurer to offer reasonable commercial terms for insurance against a standard range of insurable risks	Hard	Verify against insurance quotations.
Legal	The system should be designed, implemented, and operated in accordance with the requirements of any applicable legislation. Examples include data protection laws, laws controlling the use of cryptographic technology, laws controlling insider dealing on the stock market, and laws governing information that is considered racist, seditious, or pornographic.	Soft	Independent audit and review against security architecture capability maturity model, verification of the inventory of applicable laws to check for completeness and suitability.

404 ■ Appendix E

<i>Business Attribute</i>	<i>Attribute Explanation</i>	<i>Metric Type</i>	<i>Suggested Measurement Approach</i>
Liability-managed	The system services should be designed, implemented, and operated so as to manage the liability of the organization with regard to errors, fraud, malfunction, and so on. In particular, the responsibilities and liabilities of each party should be clearly defined.	Soft	Independent legal expert review of all applicable contracts, SLAs, etc.
Regulated	The system should be designed, implemented and operated in accordance with the requirements of any applicable regulations. These may be general (such as safety regulations) or industry-specific (such as banking regulations).	Soft	Independent audit and review against security architecture capability maturity model, verification of the inventory of applicable regulations to check for completeness and suitability.
Resolvable	The system should be designed, implemented, and operated in such a way that disputes can be resolved with reasonable ease and without undue impact on time, cost, or other valuable resources.	Soft	Independent audit and review against security architecture capability maturity model by legal experts.
Time-bound	Meeting requirements for maximum or minimum periods of time, for example, a minimum period for records retention or a maximum period within which something must be completed.	Hard	Independent functional design review against specified functional requirements.

Business Attribute	Attribute Explanation	Metric Type	Suggested Measurement Approach
Technical Strategy Attributes	<i>This group of attributes describes the need for fitting into an overall technology strategy.</i>		
Architecturally open	The system architecture should, wherever possible, not be locked into specific vendor interface standards and should allow flexibility in the choice of vendors and products, both initially and in the future.	Soft	Independent audit and review against security architecture capability maturity model of technical architecture (conceptual, logical, and physical)
COTS/GOTS compliant	Wherever possible, the system should utilize commercial off-the-shelf or government off-the-shelf components as appropriate.	Soft	Independent audit and review against security architecture capability maturity model of technical architecture (conceptual, logical, and physical).
Extendable	The system should be capable of being extended to incorporate new functional modules as required by the business.	Soft	Independent audit and review against security architecture capability maturity model of technical architecture (conceptual, logical, and physical).
Flexible and adaptable	The system should be flexible and adaptable to meet new business requirements as they emerge.	Soft	Independent audit and review against security architecture capability maturity model of technical architecture (conceptual, logical, and physical).

406 ■ Appendix E

<i>Business Attribute</i>	<i>Attribute Explanation</i>	<i>Metric Type</i>	<i>Suggested Measurement Approach</i>
Future-proof	The system architecture should be designed as much as possible to accommodate future changes in both business requirements and technical solutions.	Soft	Independent audit and review against security architecture capability maturity model of technical architecture (conceptual, logical, and physical).
Legacy-sensitive	A new system should be able to work with any legacy systems or databases with which it needs to interoperate or integrate.	Soft	Independent audit and review against security architecture capability maturity model of technical architecture (conceptual, logical, and physical).
Migratable	There should be a feasible, manageable migration path, acceptable to the business users, that moves from an old system to a new one or from one released version to the next.	Soft	Independent audit and review against security architecture capability maturity model of technical architecture (conceptual, logical, and physical).
Multisourced	Critical system components should be obtainable from more than one source to protect against the risk of the single source of supply and support being withdrawn.	Soft	Independent audit and review against security architecture capability maturity model of technical architecture at the component level.
Scalable	The system should be scalable to the size of user community, data storage requirements, processing throughput, and so on that might emerge over the lifetime of the system.	Soft	Independent audit and review against security architecture capability maturity model of technical architecture (conceptual, logical, and physical).

<i>Business Attribute</i>	<i>Attribute Explanation</i>	<i>Metric Type</i>	<i>Suggested Measurement Approach</i>
Simple	The system should be as simple as possible because complexity only adds further risk.	Soft	Independent audit and review against security architecture capability maturity model of technical architecture (conceptual, logical, and physical).
Standards compliant	The system should be designed, implemented, and operated to comply with appropriate technical and operational standards.	Soft	Independent audit and review of (1) the inventory of standards to check for completeness and appropriateness and (2) compliance with standards on the inventory.
Traceable	The development and implementation of system components should be documented so as to provide complete two-way traceability. That is, every implemented component should be justifiable by tracing back to the business requirements that led to its inclusion in the system, and it should be possible to review every business requirement and demonstrate which of the implemented system components are there to meet this requirement.	Soft	Independent expert review of documented traceability matrices and trees.

408 ■ Appendix E

<i>Business Attribute</i>	<i>Attribute Explanation</i>	<i>Metric Type</i>	<i>Suggested Measurement Approach</i>
Upgradeable	The system should be capable of being upgraded with ease to incorporate new releases of hardware and software.	Soft	Independent audit and review against security architecture capability maturity model of technical architecture (conceptual, logical, and physical).
<i>Business Strategy Attributes</i>	<i>This group of attributes describes the needs for fitting into an overall business strategy.</i>		
Brand enhancing	The system should help to establish, build, and support the brand of the products or services based upon this system.	Soft	Market surveys.
Business-enabled	Enabling the business and fulfilling business objectives should be the primary driver for the system design.	Soft	Business management focus group.
Competent	The system should protect the reputation of the organization as being competent in its industry sector.	Soft	Independent audit, focus groups, or satisfaction surveys.
Confident	The system should behave in such a way as to safeguard confidence placed in the organization by customers, suppliers, shareholders, regulators, financiers, the marketplace, and the general public.	Soft	Independent audit, focus groups, or satisfaction surveys.
Credible	The system should behave in such a way as to safeguard the credibility of the organization.	Soft	Independent audit, focus groups, or satisfaction surveys.

<i>Business Attribute</i>	<i>Attribute Explanation</i>	<i>Metric Type</i>	<i>Suggested Measurement Approach</i>
Culture sensitive	The system should be designed, built, and operated with due care and attention to cultural issues relating to those who will experience the system in any way. These issues include such matters as religion, gender, race, nationality, language, dress code, social customs, ethics, politics, and the environment. The objective should be to avoid or minimize offence or distress caused to others.	Soft	Independent audit and review of (1) the inventory of requirements in this area to check for completeness and appropriateness and (2) compliance of system functionality with this set of requirements.
Enabling time to market	The system architecture and design should allow new business initiatives to be delivered to the market with minimum delay.	Soft	Business management focus group.
Governable	The system should enable the owners and executive managers of the organization to control the business and to discharge their responsibilities for governance.	Soft	Senior management focus group, independent audit and review against security architecture capability maturity model for governance.
Providing good stewardship and custody	Protecting other parties with whom we do business from abuse or loss of business or personal information of value to those parties through inadequate stewardship on our part.	Soft	Independent audit, focus groups, or satisfaction surveys.

410 ■ Appendix E

<i>Business Attribute</i>	<i>Attribute Explanation</i>	<i>Metric Type</i>	<i>Suggested Measurement Approach</i>
Providing investment reuse	As much as possible, the system should be designed to reuse previous investments and to ensure that new investments are reusable in the future.	Soft	Independent audit and review against security architecture capability maturity model of technical architecture (conceptual, logical, physical, and component).
Providing return on investment	The system should provide a return of value to the business to justify the investment made in creating and operating the system.	Hard	Financial returns and ROI indices selected in consultation with the chief financial officer
		Soft	Qualitative value propositions tested by opinion surveys at senior management and boardroom level.
Reputable	The system should behave in such a way as to safeguard the business reputation of the organization.	Soft	Independent audit, focus groups, or satisfaction surveys.
		Hard	Correlation of the stock value of the organization versus publicity of system event history.

Appendix F: Prototype Metrics Catalog

The following table lists the information security metrics described individually in Chapter 7. We refer to it as a *prototype* metrics catalog for two important reasons: (1) the information shown here, even considering the additional text from Chapter 7, is minimal. In reality, a metrics catalog actually used by an organization would generally include a variety of extra data fields not shown here (e.g., nominal owners and audiences for all the metrics being used, information on data sources and methods of analysis and presentation/reporting), depending on what the organization finds useful; and (2) 154 metrics falls *well* short of the total number of information security metrics that would normally be considered and doesn't even account for all of the metrics mentioned in the book (many of which are merely implied). As noted in the main text, it is generally easy to generate a whole family of related metrics through minor changes to the wording or nature of any one: such variants could be listed as a group or separately, but either way, there is a real prospect of scattering near-duplicate metrics throughout the catalog unless it is so well structured that they all magically cluster together.

Rank	Reference	Example Metric	Strategic, Managerial or Operational	PRAGMATIC Ratings (%)									
				Predictive	Relevant	Actionable	Genuine	Meaningful	Accurate	Timely	Independent	Cost	Score
1	6.1	Quality of security metrics in use	S M	96	91	99	92	88	94	89	79	95	91%
2	7.1	Number of orphaned information assets without an owner	M	85	90	97	90	90	95	85	99	90	91%
3	11.1	Rate of messages received at central access logging/alerting system	O	87	88	94	93	93	94	97	89	79	90%
4	14.1	Coverage of business impact analyses	S M	95	90	99	90	95	80	86	80	88	89%
5	6.2	Percentage of security controls that may fail silently	S M O	90	90	90	90	90	93	86	93	80	89%
6	5.1	Number of security policies, standards, procedures, and metrics with committed owners	M	81	87	90	95	92	92	77	92	90	88%
7	9.1	Power consumed by the computer suite versus air conditioning capacity	O	81	69	89	92	80	99	98	90	98	88%
8	6.3	Security governance maturity	S M	95	97	70	78	91	89	90	85	90	87%
9	14.2	Business continuity management maturity	S M	90	95	70	80	90	85	90	87	90	86%

10	10.1	IT security maturity	S M	90	95	70	80	90	85	90	85	90	86%
11	12.1	Software security maturity	S M	90	95	70	80	90	85	90	85	90	86%
12	13.1	Information security incident management maturity	S M	90	95	70	80	90	85	90	85	90	86%
13	15.1	Information security compliance management maturity	S M	90	95	70	80	90	85	90	85	90	86%
14	7.2	Information asset management maturity	S M	90	95	70	80	90	85	90	85	90	86%
15	8.1	Human resources security maturity	S M	90	95	70	80	90	85	90	85	90	86%
16	9.2	Physical and environmental security maturity	S M	90	95	70	80	90	85	90	85	90	86%
17	4.1	Security risk management maturity	S M	92	98	68	78	90	83	89	84	92	86%
18	15.2	Breakdown of exceptions and exemptions	M	87	83	84	94	81	83	84	87	88	86%
19	11.2	Information access control maturity	S M	90	95	70	80	90	80	90	85	90	86%
20	4.2	Number of high/medium/low risks currently untreated/unresolved	S M O	87	87	84	81	89	80	87	83	90	85%
21	14.3	Percentage of critical business processes having adequate business continuity arrangements	M	85	97	93	84	89	75	85	75	75	85%

(continued)

Rank	Reference	Example Metric	Strategic, Managerial or Operational	PRAGMATIC Ratings (%)						
				Predictive	Actionable	Genuine	Meaningful	Accurate	Timely	
22	5.2	Security policy management maturity	S M	90	95	70	80	88	85	90
23	5.3	Traceability of policies, control objectives, standards, and procedures	M	85	89	88	90	91	87	65
24	6.4	Information security ascendency	S	97	87	15	94	86	90	99
25	5.4	Number of important operations with documented and tested security procedures	M O	95	96	91	85	95	84	62
26	14.4	Percentage of business processes having defined RTOs and RPOs	M	88	99	90	68	93	68	92
27	4.3	Information security budget variance	M	70	90	85	77	80	77	80
28	7.3	Percentage of information assets not (correctly) classified	M O	75	75	97	85	90	80	80
29	14.5	Business continuity plan maintenance status	M O	75	90	73	84	76	80	77
30	14.6	Disaster recovery test results	S M O	83	80	85	91	92	75	75
31	10.2	Percentage of systems checked and fully compliant to applicable (technical) security standards	O	81	77	89	86	89	73	74
32	8.2	Security awareness level	M O	86	89	86	82	85	80	69

33	9.3	Discrepancies between physical location and logical access location	M	75	76	72	90	82	75	85	83	60	78%
34	14.7	Uptime	M O	84	97	66	78	94	61	79	47	89	77%
35	5.5	Comprehensiveness of security policy coverage	S	75	82	92	78	80	70	73	60	81	77%
36	15.3	Number and severity of findings in audit reports, reviews, assessments, etc.	S M	79	89	87	96	92	84	30	96	36	77%
37	12.2	Percentage of controls tested realistically	M	92	95	90	65	95	60	75	55	60	76%
38	5.6	Policy coverage of frameworks, such as ISO/IEC 27002	M O	70	75	90	69	85	76	72	65	85	76%
39	7.4	Unowned information asset days	M O	40	51	84	77	74	86	92	94	82	76%
40	14.8	IT capacity and performance	S M O	92	92	82	77	96	62	84	64	29	75%
41	5.7	Number or percentage of security policies addressing viable risks	M	65	76	91	73	83	77	70	61	78	75%
42	9.4	Number of unsecured access points	M O	95	80	90	70	85	77	45	75	55	75%
43	13.2	Time taken to remediate security incidents	M	82	69	85	76	80	75	65	75	60	74%
44	15.4	Status of compliance with externally imposed information security obligations	S M O	77	85	85	70	98	68	35	89	60	74%
45	12.3	Software quality assurance	M	83	85	91	73	90	68	70	80	20	73%
46	5.8	Quality of security policies	M O	80	85	40	66	72	75	80	80	80	73%

(continued)

Rank	Reference	Example Metric	Strategic, Managerial or Operational	PRAGMATIC Ratings (%)									
				Score	Cost	Independent	Timely	Accurate	Meaningful	Genuine	Actionable	Relevant	Predictive
47	12.4	Quality of system security revealed by testing	M	83	88	83	73	90	68	80	82	10	73%
48	10.3	Time from change approval to change	M	70	71	76	90	60	84	64	60	80	73%
49	10.4	Correlation between system/ configuration logs and authorized change requests	M	87	80	90	80	80	80	60	50	47	73%
50	14.9	Mapping critical business processes to disaster recovery and business continuity plans	SM	85	92	79	81	90	70	75	40	40	72%
51	5.10	Thud factor (policy verbosity or red-tape index, waffle-o-meter)	M	82	80	60	60	70	45	85	86	84	72%
52	5.9	Percentage of policy statements unambiguously linked to control objectives	M	92	91	64	60	85	65	45	75	75	72%
53	6.5	Percentage of controls unambiguously linked to control objectives	M	92	91	64	60	85	65	45	75	75	72%
54	6.6	Number of controls meeting defined control criteria/objectives	MO	88	86	88	65	78	60	26	90	70	72%

55	10.5	Percentage of IT devices not securely configured	O	83	80	77	75	59	74	76	88	36	72%
56	10.6	Rate of change of emergency change requests	M O	64	71	69	73	78	70	70	69	83	72%
57	6.7	Percentage of critical controls consistent with controls policy	S M	83	92	80	83	89	82	32	70	35	72%
58	14.10	Business continuity expenditure	S M	75	92	20	82	95	70	70	70	70	72%
59	5.11	Number of security policies whose review/re-approval is overdue	O	54	88	92	14	97	77	43	90	89	72%
60	11.3	Days since logical access control matrices for application systems were last reviewed	M O	55	80	95	30	80	85	60	70	80	71%
61	6.9	Corporation's economic situation	S M	72	80	10	80	80	80	61	80	79	69%
62	4.4	Process/system fragility or vulnerability	S M O	90	90	44	80	92	77	66	60	22	69%
63	6.10	Percentage of controls that are ossified or redundant	S M	85	88	85	80	84	75	22	62	39	69%
64	7.5	Integrity of the information asset inventory	M O	82	66	83	78	80	43	50	66	70	69%
65	8.3	Rate of change in employee turnover or absenteeism	S M	60	66	20	85	60	80	75	80	91	69%
66	15.5	Historic consequences of noncompliance	S	70	80	72	82	80	80	20	67	65	68%
67	15.6	Number of systems whose security has been accredited	M	72	79	73	89	68	32	22	89	88	68%

(continued)

Rank	Reference	Example Metric	PRAGMATIC Ratings (%)						Score	Cost			
			Strategic, Managerial or Operational	Independent	Timely	Accurate	Meaningful	Genuine	Actionable	Predictive			
68	4.5	Number of unpatched technical vulnerabilities	M O	80	64	80	70	80	75	25	85	52	68%
69	6.11	Control objectives tied to specific business objectives	S M	96	95	65	55	99	50	40	70	40	68%
70	6.12	Days since the last serious information security incident	M	62	70	11	87	87	10	92	95	95	68%
71	11.4	Proportion of inactive user accounts that have been disabled in accordance with policy	M O	68	56	74	76	73	64	64	52	75	67%
72	5.12	Flesch readability scores for policies, procedures, standards, and guidelines	M O	68	77	60	86	35	70	64	88	41	65%
73	5.13	Number or percentage of security policies that are clear	O	75	70	68	41	96	50	56	90	34	64%
74	6.13	Annual cost of information security controls	S M	94	92	90	77	97	44	50	16	20	64%

75	10.7	Percentage of highly privileged/trusted users or functions	M O	86	80	51	40	65	39	55	95	60	63%
76	6.14	Number of different controls	S M	71	75	72	75	88	30	50	65	43	63%
77	15.7	Status of compliance with internally mandated (corporate) information security requirements	S M O	75	75	73	63	65	58	40	40	70	62%
78	13.3	Time lag between incident and detection	M O	80	70	72	30	75	50	50	65	65	62%
79	9.5	Number of unacceptable physical risks on premises	M	70	60	85	60	90	60	30	60	42	62%
80	6.15	Extent of accountability for information assets	S	94	93	78	36	72	76	30	40	37	62%
81	6.16	Information security expenditure	S M	82	94	60	60	89	29	33	49	59	62%
82	8.4	Staff morale and attitude	S M	88	72	60	75	65	75	20	50	50	62%
83	6.17	Benford's law	O	84	30	53	95	11	98	62	98	23	62%
84	15.8	Number of unapproved/unlicensed software installations identified on corporate IT equipment	M	58	55	82	73	86	47	64	66	17	61%
85	11.5	Rate of detection of access anomalies	O	83	86	65	75	70	52	44	61	11	61%
86	6.18	NPV (net present value)	M	77	72	25	35	85	55	44	60	88	60%
87	4.6	Information security risk scores	S M	72	60	55	70	71	40	60	60	50	60%
88	15.9	Percentage of security policies supported by adequate compliance activities	M	96	92	78	40	75	33	60	34	30	60%

(continued)

Rank	Reference	Example Metric	Strategic, Managerial or Operational	PRAGMATIC Ratings (%)						Score	
				Independent	Timely	Accurate	Meaningful	Genuine	Actionable	Relevant	
89	12.5	Extent to which information security is incorporated in software QA	M	85	80	67	62	70	50	35	50
90	4.7	Total liability value of untreated/ residual risks	SM	88	98	59	33	96	33	77	38
91	11.6	Logical access control matrices for applications: coverage and detail	MO	60	70	65	70	78	68	50	50
92	10.8	Entropy of encrypted content	O	78	66	23	78	3	93	74	79
93	12.6	Extent to which QA is incorporated in information security processes	M	75	70	66	61	80	50	35	36
94	8.5	Tone at the top	SM	95	50	57	40	91	45	50	25
95	6.19	Return on investment (ROI)	M	70	72	25	30	82	50	44	60
96	4.8	Coupling index	S	68	85	50	60	72	47	35	61
97	6.20	Internal rate of return (IRR)	M	69	72	25	30	82	50	44	60
98	4.9	Changes in network probe levels	MO	50	80	10	68	66	85	50	70
99	6.21	Payback period	M	65	72	25	25	88	50	44	60
100	15.10	Compliance benchmark against peers	SM	80	65	62	61	90	60	22	65

101	15.11	Number or rate of security policy noncompliance infractions detected	O	55	64	75	50	68	34	59	76	33	57%
102	6.8	Information security management customer satisfaction rating	S M	60	60	40	35	85	51	85	15	80	57%
103	12.7	Percentage of configuration items in line with service levels for performance and security	M O	60	75	65	62	40	70	35	80	20	56%
104	6.22	Information security controls coverage	M O	87	89	65	40	74	35	46	40	30	56%
105	13.4	Percentage of incidents for which root causes have been diagnosed and addressed	M	85	85	67	40	77	40	48	16	40	55%
106	4.10	Organizational and technical homogeneity	M O	67	70	40	59	67	50	33	65	45	55%
107	10.9	Percentage of IT/process changes abandoned, backed-out, or failed for information security reasons	M O	50	70	55	60	65	40	50	45	60	55%
108	6.23	DEFCON level	M	5	10	30	85	25	71	88	90	91	55%
109	10.10	Vulnerability index	O	74	85	71	74	60	32	46	33	19	55%
110	8.6	Corporate security culture	S M	60	76	55	75	60	60	10	75	20	55%
111	8.7	System accounts-to-employees ratio	M O	74	67	38	39	68	42	36	83	44	55%
112	15.12	Embarrassment factor	S M	26	38	20	50	63	72	40	87	87	54%
113	5.14	Percentage of security policies that satisfy documentation standards	M O	66	47	79	45	74	38	44	50	35	53%
114	6.24	Controls consistency	M	78	83	67	60	71	33	27	31	27	53%

(continued)

Rank	Reference	Example Metric	Strategic, Managerial or Operational	PRAGMATIC Ratings (%)						Score	
				Predictive	Relevant	Actionable	Genuine	Meaningful	Accurate	Timely	
115	8.8	Opinion surveys and direct observations of the culture	S M	80	80	60	55	75	55	10	45
116	6.25	Scope of information security activities	S	86	74	35	44	70	37	30	44
117	7.6	Value of information assets owned by each information asset owner	M	48	64	78	57	79	38	50	22
118	5.15	Number of security policies that are inconsistent with other policies or obligations	O	60	49	76	43	88	45	41	43
119	11.7	Logical access control matrices for applications: state of development	M O	70	50	60	60	88	25	40	20
120	12.8	Percentage of technical controls that fail safe	M	59	55	66	78	77	33	20	48
121	12.9	Number of deviations identified between configuration repository and actual asset configurations	M O	50	60	60	64	40	50	40	60
122	13.5	Cumulative costs of information security incidents to date	S M	76	85	0	30	95	30	33	40

123	15.13	Percentage of purchased software that is unauthorized	M	71	51	90	75	82	35	13	20	6	49%
124	13.6	Number of information security events and incidents, major and minor	S M O	70	60	0	50	72	35	35	70	50	49%
125	7.7	Percentage of information assets not marked with the (correct) classification	O	52	53	63	44	62	13	17	87	44	48%
126	11.8	Quality of identification and authentication controls	M	60	87	40	40	56	36	41	22	42	47%
127	10.11	Delays and inconsistencies in patching	O	43	41	77	62	36	32	48	34	42	46%
128	15.14	Proportionality of expenditure on assurance versus potential impact × likelihood	M	65	40	85	40	3	20	46	76	35	46%
129	15.15	Percentage of software licenses purchased but not accounted for in repository	M O	1	1	90	84	1	70	50	81	30	45%
130	14.11	Percentage of critical systems reviewed for compliance with critical control requirements	O	62	53	68	36	5	69	34	43	33	45%
131	11.9	Proportion of business units that have proven their identification and authentication mechanisms	M	69	73	72	32	36	4	56	2	50	44%
132	9.6	Distance between employee and visitor parking	O	1	0	6	93	2	93	66	45	66	41%
133	10.12	Perceptions of rate of change in IT	M	40	50	6	65	70	50	30	14	40	41%

(continued)

Rank	Reference	Example Metric	Strategic, Managerial or Operational	PRAGMATIC Ratings (%)						Score	
				Predictive	Relevant	Actionable	Genuine	Meaningful	Accurate	Timely	
134	4.11	Percentage of controls working as defined	M O	62	62	44	26	66	25	22	36
135	4.12	Organization's insurance coverage versus annual premiums	S	64	46	5	25	20	16	10	82
136	8.9	Help desk security traffic volumes	O	24	33	16	58	5	35	33	45
137	6.26	Value at risk (VAR)	M	70	65	20	30	35	40	30	30
138	8.10	Culture/worldview	S M	66	30	10	70	40	56	15	40
139	11.10	Number of times that assets were accessed without authentication or validation	O	61	78	33	16	33	0	44	35
140	10.13	Patching policy compliance	O	66	52	55	77	19	36	11	8
141	8.11	Employee turn versus account churn	O	30	30	11	36	44	36	62	57
142	6.27	Return on security investment (ROSI)	M	40	40	20	20	55	45	25	40
143	8.12	Organizational dysfunction	S M	75	20	10	60	80	40	15	10

144	13.7	Number of information security incidents that could have been prevented, mitigated, or avoided	M	50	75	0	15	85	5	16	9	42	33%
145	15.16	Percentage of critical information assets residing on fully compliant systems	M	48	26	36	41	56	13	19	46	12	33%
146	13.8	Nonfinancial impacts of incidents	S M	60	65	0	20	60	6	30	20	17	31%
147	8.13	Psychometrics	M O	40	24	0	79	15	55	10	42	5	30%
148	9.7	Percentage of facilities that have adequate external lighting	O	2	5	70	42	11	46	35	18	31	29%
149	10.14	Number of changes	O	55	24	9	6	2	3	15	26	67	23%
150	6.28	Security budget as percentage of IT budget or turnover	M	13	3	16	2	2	0	4	18	88	16%
151	10.15	Number of viruses detected in user files	O	8	13	6	11	3	2	5	5	78	15%
152	10.16	Number of firewall rules changed	O	2	1	1	10	2	33	14	4	17	9%
153	4.13	Number of attacks	M	13	9	1	2	12	1	4	1	7	6%
154	10.17	Toxicity rate of customer data	O	0	0	0	0	0	0	0	0	0	0%

Free ebooks ==> www.ebook777.com

Appendix G: Effect of Weighting the PRAGMATIC Criteria

Below, we compare the 30 top-scoring metrics, first unweighted (every rating has the same weight), and then with the following weightings: **Predictive**, 25%; **Relevant**, 20%; **Actionable**, 9%; **Genuine**, 3%; **Meaningful**, 5%; **Accurate**, 8%; **Timely**, 7%; **Independent**, 3%; **Cost**, 20%.

Metric	Unweighted Score	Metric	Weighted Score
Quality of security metrics in use	91%	Quality of security metrics in use	93%
Number of orphaned information assets without an owner	91%	Coverage of business impact analyses	91%
Rate of messages received at central access logging/alerting system	90%	Security governance maturity	90%
Coverage of business impact analyses	89%	Number of orphaned information assets without an owner	90%
Percentage of security controls that may fail silently	89%	Security risk management maturity	89%

<i>Metric</i>	<i>Unweighted Score</i>	<i>Metric</i>	<i>Weighted Score</i>
Number of security policies, standards, procedures, and metrics with committed owners	88%	Percentage of business processes having defined RTOs and RPOs	89%
Power consumed by the computer suite versus air conditioning capacity	88%	Business continuity management maturity	88%
Security governance maturity	87%	IT security maturity	88%
Business continuity management maturity	86%	Software security maturity	88%
IT security maturity	86%	Information security incident management maturity	88%
Software security maturity	86%	Information security compliance management maturity	88%
Information security incident management maturity	86%	Information asset management maturity	88%
Information security compliance management maturity	86%	Human resources security maturity	88%
Information asset management maturity	86%	Physical and environmental security maturity	88%
Human resources security maturity	86%	Percentage of security controls that may fail silently	88%
Physical and environmental security maturity	86%	Rate of messages received at central access logging/alerting system	88%
<i>(continued)</i>			

<i>Metric</i>	<i>Unweighted Score</i>	<i>Metric</i>	<i>Weighted Score</i>
Security risk management maturity	86%	Information access control maturity	88%
Breakdown of exceptions and exemptions	86%	Security policy management maturity	88%
Information access control maturity	86%	Information security ascendency	87%

Free ebooks ==> www.ebook777.com

Appendix H: ISO27k Maturity Scale Metrics

The tables that follow can be used to assess and score the maturity of an organization's approach to information security against a broad range of information security practices recommended by ISO/IEC 27002:2005.

The assessment criteria make the scoring process more objective and repeatable than it would otherwise be. However, the scoring is best conducted by someone with an information security or IT audit background who either knows the organization inside-out or has access to the people who do and preferably both. Consider one row at a time, determining which of the stated criteria offer the best fit, and identify the percentage score accordingly, interpolating between the scoring points where appropriate. Make notes about the scoring, including any evidence, incidents, situations, or concerns that were particularly influential—you may be asked to explain or justify particular scores later, and most of us find it difficult to remember all the scoring decisions without our notes.

Tip: Although this appendix reflects the ISO27k standards, it is *not* comprehensive. The scoring indicators do not incorporate all of the security issues and controls explicitly recommended by the standard. The tables are provided as templates or starting points from which you are encouraged to develop your own customized suite of scoring scales, but bear in mind the trade-offs between simplicity/complexity, cost, accuracy, speed of use, and utility. Our primary aim in this book is to help you develop worthwhile information security metrics, not to conduct a detailed analysis of your organization's security status.

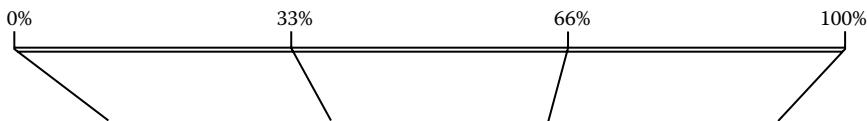
For summary-level metrics, the scores can then simply be averaged in each section and overall for a grand total score. The criteria and the sections may optionally be weighted first because some controls are more important than others—we leave this as an exercise for the reader.

The individual ratings for each row in the tables, along with your notes and perhaps the evidence you gathered, may prove useful for information security professionals tasked by management with improving the scores.

As well as using the maturity scale method to score small organizations or individual departments and facilities directly, we have used a more detailed version of the matrix to assess large organizations' compliance with the ISO27k standards. The method involves a team of qualified IT auditors assessing, scoring, comparing, and contrasting business units using common criteria similar to those shown here plus an accompanying ISO27k audit checklist. It works extremely well and has proved popular with management.

By the way, please do not assume that 100% is the target or ideal score in every case or, for that matter, that 0% is necessarily an outright fail. Risk analysis is an integral part of the ISO27k approach, and your risks (and, hence, the appropriate controls) are not the same as everyone else's. These are entirely generic scoring scales. Some controls might not be appropriate in your organization, and others might not go far enough.

Tip: If you are blessed with a progressive management, the scores lend themselves to the publication of corporate league tables that motivate underperforming business units to review their approach to information security and encourage the transfer of good practices from their better peers. Be aware, however, that bad scores can generate serious resentment, so be careful if you take this approach—you might, for example, offer underperforming business units a grace period to get their act together before reassessing them and publishing the numbers.

ISO/IEC 27002 Section 4: Security Risk Management Maturity Metrics

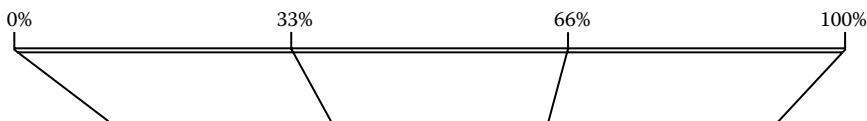
<i>No Information Security Risk Management</i>	<i>Basic Information Security Risk Management</i>	<i>Good Information Security Risk Management</i>	<i>Excellent Information Security Risk Management</i>
There are no information security risk-related policies, procedures, standards, guidelines, or similar documents of any description.	There are a few information security risk-related policies, procedures, etc., but they are incomplete, not fully up to date, and not necessarily authorized by management.	There is a suite of information security risk-related policies, procedures, guidelines, etc. with no significant gaps, up to date, and properly authorized by management.	A comprehensive, high-quality suite of information security risk-related strategies, policies, procedures, standards, and guidelines has been duly mandated by management.
Information security risk tolerance or appetite is undefined.	Information security risk tolerance or appetite is partially defined.	Information security risk tolerance or appetite is defined in some form.	Information security risk tolerance or appetite is defined and formally documented.
Information security risks are neither identified nor analyzed.	Some information security risks are identified and analyzed, but there are substantial doubts about the coverage and quality of the analysis.	Most information security risks, including all key risks, are identified and analyzed or quantified systematically.	Information security risks are identified and analyzed or quantified rigorously, systematically, and comprehensively.

434 ■ Appendix H



<i>No Information Security Risk Management</i>	<i>Basic Information Security Risk Management</i>	<i>Good Information Security Risk Management</i>	<i>Excellent Information Security Risk Management</i>
No information security risk inventory, list, database, or records of any description exist.	Partial information security risk inventory is not entirely complete, accurate, and up to date and not necessarily all in one place or form.	Substantially complete and accurate information security risk inventory is periodically updated and maintained with occasional, ad hoc audits or reviews.	Complete, accurate, and highly reliable information security risk inventory is routinely maintained and routinely audited.
Information security risks are wholly untreated (any security controls are not explicitly linked to identified risks).	Some information security risks are treated, but many more are left to chance and the treatments are not entirely appropriate and complete.	Most information security risks, including all key risks, are treated appropriately and brought within defined risk-tolerance levels.	All information security risks are properly treated to bring them within management's risk tolerance as confirmed by audits and reviews.

ISO/IEC 27002 Section 5: Security Policy Management Process Maturity Metrics



<i>No Information Security Policy Management</i>	<i>Basic Information Security Policy Management</i>	<i>Reasonable Information Security Policy Management</i>	<i>Excellent Information Security Policy Management</i>
There is nothing even remotely resembling a security policy as such.	There is a security policy of sorts although probably of poor quality (e.g., badly worded or inconsistent), incomplete, or out of date with some elements undocumented.	The information security policy is documented, reasonably complete, accurate, and up to date, reflecting most corporate and external obligations, albeit somewhat stilted and difficult to read and apply in places and perhaps with limited coverage on topical issues, such as cloud computing.	The information security policy materials are formalized, entirely complete, accurate, up to date, consistent, and readable, explicitly reflecting a documented set of high-level security principles, fully reflecting all corporate and external obligations and promoting generally accepted good security practices.
There are no information security procedures, standards, guidelines, etc. to speak of.	There are some information security procedures, guidelines, etc., but they are inconsistent, incomplete, and generally shabby and in need of substantial revision.	The information security procedures, standards, guidelines, etc. are of a reasonable quality in all important respects, including coverage and consistency, but with some room for improvement.	There is a comprehensive, well-written suite of procedures, standards, guidelines, and training materials supporting the information security policy and, in turn, the organization's obligations and objectives for information security.

436 ■ Appendix H

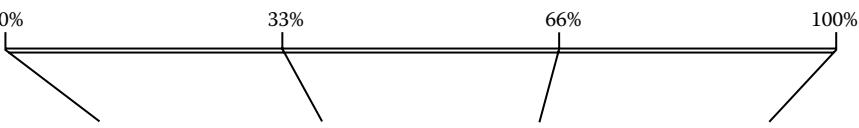


<i>No Information Security Policy Management</i>	<i>Basic Information Security Policy Management</i>	<i>Reasonable Information Security Policy Management</i>	<i>Excellent Information Security Policy Management</i>
Nobody feels the slightest compulsion to own or manage the information security policy materials.	Someone accepts responsibility for the information security policy materials, perhaps grudgingly and informally, and is not entirely clear what that means.	There is a designated owner for the information security policy materials with, at least, the key responsibilities laid down in some form.	There is a formally designated and competent owner for the information security policies whose responsibilities are fully documented and accepted.
There is nothing in the way of a policy for management to review or approve, and it doesn't even appreciate that there ought to be.	The security policy materials are not all properly authorized, at least, not recently and not consistently.	The information security policy has been formally approved by management at some point within the past year or two.	The policy materials have been formally reviewed and mandated by senior management with evidence of regular review, maintenance, and re-approval of the suite.

ISO/IEC 27002 Section 6: Security Governance Maturity Metrics

<i>No Information Security Governance</i>	<i>Basic Information Security Governance</i>	<i>Good Information Security Governance</i>	<i>Excellent Information Security Governance</i>
There is essentially no information security management, let alone an information security management system (ISMS).	A bare-bones ISMS exists with a minimal organizational structure, limited management support, and a passing resemblance to the ISO27k standards.	An ISMS reflects and is believed to comply to a large extent with the key requirements of ISO/IEC 27001, although it's not currently certified as such.	The ISMS is currently certified fully compliant with ISO/IEC 27001 by a recognized and accredited certification body.
Management has no clue about information security and is patently not interested in this field: there is no management support for information security, perhaps even hostility toward it.	Management has some concerns about information security but generally seems content to let it drift along under middle or lower management with minimal support and funding.	Management takes a genuine interest in information security, providing some direction and guidance, identifying someone to be responsible for it, and providing a security budget.	Management fully supports information security, making it crystal clear that it is an essential corporate function by assigning it explicitly to a senior manager or director with a generous budget.

438 ■ Appendix H



The diagram shows a horizontal scale with arrows pointing downwards from the numbers 0%, 33%, 66%, and 100%. The scale is represented by a thin horizontal line with tick marks at each percentage point.

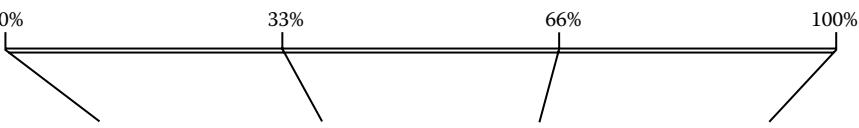
<i>No Information Security Governance</i>	<i>Basic Information Security Governance</i>	<i>Good Information Security Governance</i>	<i>Excellent Information Security Governance</i>
There are no information security metrics; information security is simply not measured at all.	There is a random assortment of information security metrics, but they are not much use to anyone, and most wouldn't really be missed if they mysteriously disappeared one day.	There are a few good information security metrics, regularly reported and generally anticipated by management that uses them routinely; there are some gaps or overlaps, however, and no security measurement system as such.	There is an outstanding <i>information security measurement system</i> in place, comprehensive in scope, properly specified, well designed and implemented, PRAGMATIC, and highly effective in practice.
There is no "security person" because nobody would accept that their role includes information security; nobody expresses the slightest interest in this area; everyone points at someone else.	Somebody informally accepts their role in managing information security, but the details are uncertain; they may not be properly qualified or sufficiently experienced, and they probably have other, more pressing duties.	There is an information security manager or the equivalent; at least one suitably qualified and experienced person is assigned to information security activities, and there is some structure to the function, including its relationships to other functions, such as IT, risk management, and compliance.	There is a CISO or the equivalent who leads and is supported by a full complement of suitably qualified and experienced information security professionals; relationships to other functions are highly effective (e.g., regular meetings, reports circulated, activities coordinated).



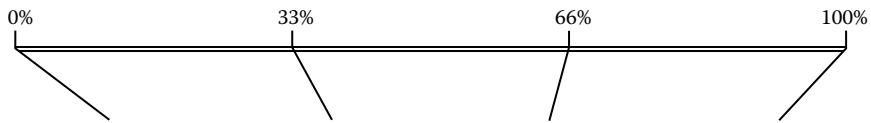
The diagram shows a horizontal scale at the top with four tick marks labeled 0%, 33%, 66%, and 100%. Three vertical lines extend downwards from the 33%, 66%, and 100% marks, each pointing to the bottom of one of the four rows in the table below.

<i>No Information Security Governance</i>	<i>Basic Information Security Governance</i>	<i>Good Information Security Governance</i>	<i>Excellent Information Security Governance</i>
Nobody has any information security roles and responsibilities.	While some people have information security responsibilities, they are not necessarily documented or associated with specific security roles.	Many information security responsibilities, including all the key ones, are documented in job descriptions, etc. corresponding to roles that are filled by suitable people.	Information security roles and responsibilities are fully documented and assigned to suitable professionals with evidence that these are periodically checked and, where necessary, updated.
There are no links or reference to external parties on information security matters: everything to do with information security (such as it is) is handled internally.	Occasionally there are hookups with external parties on information security matters, but the liaisons tend to focus on dealing with very specific issues and don't persist.	There is fairly regular contact (e.g., every month or so) with external parties on information security matters, including informal sharing of good practices as well as dealing with joint concerns.	There is frequent, close contact, both formal (including regular liaisons or meetings) and informal, with a wide variety of external parties on all manner of information security and related matters.

440 ■ Appendix H

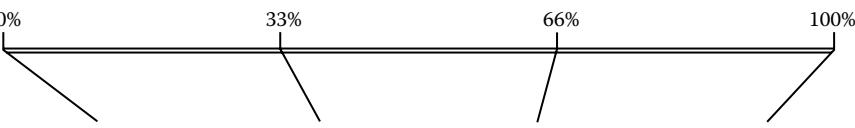


<i>No Information Security Governance</i>	<i>Basic Information Security Governance</i>	<i>Good Information Security Governance</i>	<i>Excellent Information Security Governance</i>
Information security risks relating to or arising from third parties are essentially unknown.	Information security risks relating to or arising from third parties are partially recognized but largely unmanaged.	Most information security risks relating to or arising from third parties, including all the key ones, are recognized, analyzed, and treated appropriately, for example, through nondisclosure agreements.	All information security risks relating to or arising from third parties are comprehensively and proactively monitored and maintained within acceptable limits, for example, through risk avoidance, formal contractual liabilities, SLAs, and active relationship management.

ISO/IEC 27002 Section 7: Information Asset Management Maturity Metrics

<i>No Information Asset Management</i>	<i>Basic Information Asset Management</i>	<i>Good Information Asset Management</i>	<i>Excellent Information Asset Management</i>
There is no record of information assets in any form.	A few information assets are listed somewhere, but the lists are incomplete, out of date, and inconsistent.	A list or inventory of some information assets, including most of the important ones, is maintained in a reasonably complete, accurate, and up-to-date state.	A comprehensive database accurately and completely records details of most information assets, including all the important ones, and it is periodically audited and actively maintained by a suitable owner.
“Information asset owner—what on earth are you going on about now?”	Some information assets notionally belong to someone, although most owners probably don’t appreciate what that actually means in practice, and there is no formality to the process.	“Information asset owner” is a defined and recognized term, used in policies and procedures, etc.; owners have been identified for the most important information assets, and they have at least a reasonable understanding of the associated security obligations, albeit perhaps a bit unclear on the true meaning of accountability.	It is straightforward to identify the owners of all important information assets because they have been formally nominated by management; the owners understand and willingly accept personal accountability for adequately protecting their assets.

442 ■ Appendix H



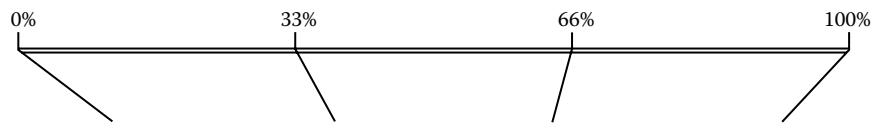
The diagram shows a horizontal scale at the top with four tick marks labeled 0%, 33%, 66%, and 100%. Three vertical lines extend downwards from the 33%, 66%, and 100% marks, each pointing to the middle of the first, second, and third rows of the table respectively.

<i>No Information Asset Management</i>	<i>Basic Information Asset Management</i>	<i>Good Information Asset Management</i>	<i>Excellent Information Asset Management</i>
Security controls bear little, if any, relationship to the risks associated with information assets; it is as if they have been selected and applied at random.	Security controls are vaguely aligned with the risks associated with information assets, but there are definite inconsistencies.	Most security controls directly reflect the risks associated with information assets with key information assets being consistently protected.	All security controls are explicitly required either by baseline security policies and standards or to address risks formally identified through risk analysis.
Information assets are not classified at all; there is no classification scheme.	Some information assets are classified, but they are not always identified consistently nor properly marked and secured.	Most information assets, including all the important ones, are appropriately classified and marked, but some are underprotected or overprotected.	Classifications are used consistently, routinely, and formally to separate different categories of information without exception.

ISO/IEC 27002 Section 8: Human Resources Security Maturity Metrics

<i>No Human Resources Security</i>	<i>Basic Human Resources Security</i>	<i>Good Human Resources Security</i>	<i>Excellent Human Resources Security</i>
Information security roles and responsibilities are entirely undocumented.	Some information security roles and responsibilities are documented, though not very well or consistently.	Most information security roles and responsibilities, including all the important ones, are assigned to individuals through being incorporated into vacancy notices, job descriptions, and codes of conduct.	Information security roles and responsibilities are comprehensively documented, formally assigned to suitable individuals (typically in legally binding contracts of employment or terms and conditions of employment), and are proactively maintained (e.g., periodically reconfirmed with the individual's signature to confirm his or her acceptance).

444 ■ Appendix H



<i>No Human Resources Security</i>	<i>Basic Human Resources Security</i>	<i>Good Human Resources Security</i>	<i>Excellent Human Resources Security</i>
<p>It does not even occur to management that candidates and employees might not be entirely trustworthy, so no background checks are performed.</p>	<p>New employees may be security-screened where their roles are obviously sensitive or trusted, but the processes are weak and inconsistent; most candidates undergo minimal accuracy checks on their CVs/résumés, if anything.</p>	<p>New employees are routinely security-screened prior to employment, especially for sensitive or trusted roles, using a documented screening process or background checks, such as taking up references, verifying their claimed identities and qualifications, plus credit checks where permitted; any subsequent checks tend to be ad hoc.</p>	<p>Prospective employees are routinely security-screened, background checked, or positively vetted according to the nature of their roles, prior to interview and periodically thereafter during employment, including prior to being promoted or transferred.</p>
<p>It does not even occur to management that contractors, consultants, temps, and other third parties might not be entirely trustworthy, so no background checks are performed.</p>	<p>Contractors, consultants, temps, and other third parties may be security-screened where their roles are obviously sensitive or trusted, but the processes are weak and inconsistent.</p>	<p>Contractors, consultants, temps, and other third parties are routinely security screened, especially for sensitive or trusted roles, whether directly by the organization or by their employers.</p>	<p>Contractors, consultants, temps, and other third parties are generally not permitted, but if they are used at all, they are security-checked by the organization to the same degree and in the same manner as employees.</p>



<i>No Human Resources Security</i>	<i>Basic Human Resources Security</i>	<i>Good Human Resources Security</i>	<i>Excellent Human Resources Security</i>
There are no information security awareness, training, or educational activities.	Basic information security awareness, training, or educational activities take place sporadically and infrequently.	Some information security awareness, training, or educational activities take place, especially for security-related roles, with some regular activities (e.g., quarterly updates).	A comprehensive managed program of information security awareness, training, and educational activities takes place with a constant drip-feed of creative, engaging materials aimed at all applicable audiences.
Information security is never a disciplinary matter.	Employees or third parties may occasionally be warned for information security infractions, but they are unlikely to be dismissed.	Employees or third parties who commit information security infractions are subject to formal disciplinary processes potentially including dismissal and prosecution.	Employees or third parties who commit information security infractions are seriously at risk of being shot, let alone disciplined, fired, or prosecuted.

446 ■ Appendix H



The diagram shows a horizontal line with arrows at both ends. Above the line are the percentages 0%, 33%, 66%, and 100%. Three vertical lines extend downwards from the 0%, 33%, and 66% marks, pointing to the top edge of the table rows.

<i>No Human Resources Security</i>	<i>Basic Human Resources Security</i>	<i>Good Human Resources Security</i>	<i>Excellent Human Resources Security</i>
There are no last-day formalities when employees or third parties end their working relationships with the organization (resignations or dismissals).	Employees may be taken through some sort of exit interview (mostly following dismissals), but the process tends to be informal and inconsistent and has little information security content; third parties generally just return from whence they came; user IDs are usually terminated at some point.	There is a formal exit interview process for most employees and third parties, especially for those leaving security-relevant roles or having access to valuable information assets or anyone dismissed for security reasons; some job-changers may be put through a similar process; user IDs and access rights are routinely reviewed.	There is a formal, structured exit interview process for all leavers and most job-changers, in which information security plays a substantial part (e.g., reclaiming information assets, credentials, etc., withdrawing all access rights, and reminding them of their ongoing security obligations).
Leavers simply leave with no regard to any information assets they may possess or have come into contact with.	Leavers are generally requested to return corporate information assets, but often it is not known what they have, and nobody checks up.	Leavers are required to return all corporate information assets, perhaps in order to receive their final pay packet; managers are expected to check up.	Leavers' possession of, access to, control over and knowledge of information assets is addressed appropriately; home visits may be needed to search for and retrieve classified materials.

ISO/IEC 27002 Section 9: Physical and Environmental Maturity Metrics

<i>No Physical and Environmental Controls</i>	<i>Basic Physical and Environmental Controls</i>	<i>Good Physical and Environmental Controls</i>	<i>Excellent Physical and Environmental Controls</i>
The campus, site, facilities, buildings, etc. are completely open with unrestricted public access permitted or readily available to all areas.	There are some restricted areas but not necessarily consistently defined and controlled, for example, the receptionists who are expected to do office security are inadequately trained and are not on duty around the clock; there is a lot of faith in remaining hidden or obscure or in deterring intruders, thieves, vandals, and saboteurs.	Restricted areas are properly defined and secured in most cases, for example, using professional security guards on duty 24/7 with suitable walls, barriers, locks, CCTV, intruder alarms, etc.	Physical access to all information assets is strictly controlled according to the specific classification or needs assessments with multiple overlapping and complementary layers of control (e.g., armed guards; blanket CCTV; alarms; absolutely no unaccompanied access to sensitive facilities; and special controls for visitors, delivery areas, and loading bays).

448 ■ Appendix H



No Physical and Environmental Controls	Basic Physical and Environmental Controls	Good Physical and Environmental Controls	Excellent Physical and Environmental Controls
There is no fire or smoke protection, for example, alarms, suppression, procedures, etc.; there are almost certainly combustible materials and sources of ignition, but management is blithely unaware of, or underplays or ignores, the risks.	Fire and smoke protection is minimal, for example, manual extinguishers, basic procedures, etc., but it is inconsistently applied and somewhat unreliable; it may not even meet statutory health and safety or building code requirements.	Fire and smoke protection is generally adequate, including suitable fire and smoke barriers, removal of unnecessary combustible materials and ignition sources, automated fire and smoke alarms, and suppression, regular evacuation exercises, etc., giving appropriate fire protection to most information assets particularly the most valuable or critical.	Fire and smoke protection for the entire facility is outstanding, having been professionally designed, installed, and maintained with particular attention paid to protecting valuable collections of information assets, such as people, computer rooms, cables, archive stores, and storage media generally.



<i>No Physical and Environmental Controls</i>	<i>Basic Physical and Environmental Controls</i>	<i>Good Physical and Environmental Controls</i>	<i>Excellent Physical and Environmental Controls</i>
No flood or leak protection, leaving substantial flood and leak risks unmitigated.	Minimal flood and leak protection is in place, but it is inconsistently applied, does not entirely reflect the risks, and is generally inadequate to prevent or mitigate serious floods and water damage affecting vulnerable information assets.	Flood and leak protection is in place for the most valuable and vulnerable information assets, at least, for example, having selective water barriers, water-detection and alarm systems plus suitable flood response procedures, and plastic sheeting and mops available.	Excellent flood and leak protection is applied to all information assets, for example, professionally designed, installed, and maintained waterproof equipment, suitable water barriers, leak detection alarms, regular inspections and preventive maintenance, and well-practiced incident response procedures.
No air conditioning leaves substantial risks of overheating.	Minimal air conditioning is barely able to cope with the heat load created by IT and other equipment.	Professionally designed, installed, managed, and maintained air-conditioning equipment is suitable for its intended purpose in terms of reliability and capacity to support critical information systems at least.	Exemplary computer-grade air-conditioning with spare capacity and redundant units is available with routine monitoring, preventive maintenance, and incident response procedures, etc. protecting all vulnerable information systems.

450 ■ Appendix H



No Physical and Environmental Controls	Basic Physical and Environmental Controls	Good Physical and Environmental Controls	Excellent Physical and Environmental Controls
No specific controls over electrical power exist for ICT equipment; if the main power fails, critical systems will fail more or less immediately.	Basic power protection, such as surge arrestors and small UPS for some IT systems (hopefully but not necessarily all the critical ones) exist, well short of being a comprehensive power architecture leaving substantial risks of power failures, brownouts, surges, etc. and probably a history of power incidents (though maybe not recorded in any formal way).	Suitable power protection for most IT systems, including all critical systems, using surge arrestors, UPS, capacity monitoring, occasional tests, etc. exists with some evidence of the power arrangements having been professionally designed and installed, but there may be a few serious power incidents on record.	Clear evidence of a professionally implemented power architecture giving excellent power protection for all IT systems, using generator-backed UPS with adequate fuel, redundant feeds, preventive maintenance, regular on-load tests, routine power monitoring with alarms, etc. exists; there have been no serious incidents ever and few, if any, minor incidents.



<i>No Physical and Environmental Controls</i>	<i>Basic Physical and Environmental Controls</i>	<i>Good Physical and Environmental Controls</i>	<i>Excellent Physical and Environmental Controls</i>
Cabling and IT equipment is left to fend for itself.	Minimal physical protection for cabling and equipment exist; maintenance and repairs generally follow incidents.	All critical cables and items of equipment are well protected in secure cabinets, ducts/conduits, alarms, etc.; most other information assets are protected to a suitably defined baseline level at least; occasional checks and some preventive maintenance are done.	All cables, items of equipment, essential tools, storage media, etc., are fully protected physically according to the classification or individual needs assessments as confirmed by regular inspections and preventive maintenance.
Off-site IT equipment and media is "out of sight, out of mind."	Off-site IT equipment and media is supposed to be appropriately secured, but the controls are quite weak and remain unchecked; information assets can easily be taken off-site without proper authority or registration.	Off-site IT equipment and media is secured according to the requirements specified by the applicable information asset owners and mandatory baseline security standards; there are strong procedures for taking information assets off-site.	The security of off-site IT equipment and media, where permitted at all, is routinely checked for compliance with documented security requirements by unannounced site inspections, random bag and vehicle checks, metal detectors, x-ray machines, etc.

452 ■ Appendix H



No Physical and Environmental Controls	Basic Physical and Environmental Controls	Good Physical and Environmental Controls	Excellent Physical and Environmental Controls
Redundant (and in some cases, current) storage media and IT equipment mysteriously disappears without a trace, sometimes turning up unexpectedly in public.	Redundant storage media and IT equipment is supposed to be disposed of properly, but the controls are quite weak and compliance largely optional.	There are procedures for secure disposal of storage media and IT equipment that contains sensitive or valuable information content with shredders, etc. being readily available and occasional compliance checks being made by managers; commercial disposal services may be used.	Highly sensitive/valuable information content is strongly encrypted; hence, secure disposal is not as critical as it might appear; nevertheless, there are strict procedures for securely disposing of all information assets, for example, cross-cut shredders, incinerators, degaussers, and destruction of redundant or failed equipment either on site or by certified secure disposal specialists; disposals are routinely monitored and recorded in asset registers.

ISO/IEC 27002 Section 10: IT Security Maturity Metrics*

<i>No IT Security</i>	<i>Basic IT Security</i>	<i>Good IT Security</i>	<i>Excellent IT Security</i>
No operating procedures are in place.	Some operating procedures, partially documented, are in place.	Most operating procedures, including all the important security-related ones, are documented.	All procedures are well documented, supporting the associated policies and supported by guidelines, etc.
No segregation of duties exists.	A few incompatible duties are segregated between individuals.	Most incompatible duties are segregated between competent individuals.	All incompatible duties are carefully segregated between competent individuals; security is reinforced with access controls and logging.
Development, test, and operational systems are one big mess, sharing the same hardware and networks.	Some isolation between operational and other systems exists, but some points of contact or crossover are not entirely controlled.	Operational, test, and development systems are segregated with change control procedures governing promotion to operational status.	Development, test, and operational systems are totally isolated and separate with strict change control procedures governing movements between them.

* ISO/IEC 27002:2005 calls this section "Communications and operations management."

454 ■ Appendix H



<i>No IT Security</i>	<i>Basic IT Security</i>	<i>Good IT Security</i>	<i>Excellent IT Security</i>
IT services are outsourced without a care, for example, public cloud services used for sensitive or critical business IT.	Security aspects of outsourced IT services are partially covered by contracts and agreements but not comprehensive (e.g., limited change and incident management).	Security aspects of outsourced IT services are fully covered by suitable contracts and agreements with some compliance measures and relationship management.	Few, if any, IT services are outsourced with strict contractual terms plus compliance measures, liabilities/penalties for nonperformance, and proactive relationship management.
IT systems and services are implemented recklessly or chaotically.	IT systems and services are implemented with some care, but security issues, such as capacity and performance, are not well managed.	IT systems and services are implemented carefully following documented procedures, taking due account of capacity, performance, and other aspects of operational security, such as access rights and backups.	IT systems and services are rarely implemented, following comprehensive and strictly worded plans, policies, and procedures taking full account of security aspects.
No malware protection exists; malware incidents are commonplace, but many remain unrecognized.	Some malware protection exists, but gaps in the defenses have led to malware incidents being identified.	Strong, multilayered malware protection leads to rather few malware incidents.	Highly effective malware protection exists, including source code malware analysis for new applications.



<i>No IT Security</i>	<i>Basic IT Security</i>	<i>Good IT Security</i>	<i>Excellent IT Security</i>
No backups or archives exist.	Some backups and archives exist, but they are somewhat incomplete, disorganized, sporadic, and unreliable; they generally live on site, often in ordinary cupboards or cardboard boxes; the ability to restore data is only ever checked under duress when the original data have been lost.	Structured, regular backups and archives exist, including data, programs, and configurations, proven by occasional test restores with duplicates of critical backups and archives stored off-site; some cross-training of people for critical roles is done.	Dedicated backup and archive systems, procedures, and professionals, regularly proven, exist with secure off-site storage as a rule plus secure on-site duplicates for speed of access; competent deputies and understudies for all critical people are employed, plus routine multi-skilling.

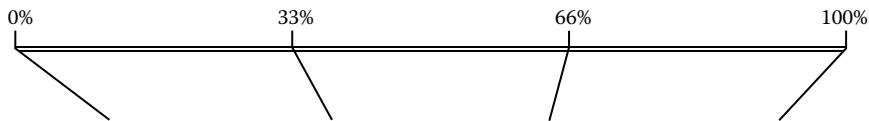
456 ■ Appendix H



<i>No IT Security</i>	<i>Basic IT Security</i>	<i>Good IT Security</i>	<i>Excellent IT Security</i>
Network security is unmanaged, often unmanageable, in fact; most network security incidents are neither recognized as such nor addressed.	Some efforts are made to manage network security (e.g., access to network services controlled) and deal with at least some of the many network security incidents.	Network security is professionally managed with few incidents; most network services and equipment (including all critical ones) are secured to some extent (e.g., fallback links for critical connections); network incidents are routinely investigated, particularly the more serious ones.	Exemplary security arrangements control all network services, links, and equipment (e.g., multiple redundant links); 24/7 network security monitoring and management is done by competent and experienced professionals; very few network security incidents occur, all thoroughly investigated and resolved.
Storage media is unmanaged.	Some storage media is partially controlled (e.g., basic media handling procedures for tapes and disks but not papers and USB sticks), but most remains uncontrolled.	Most storage media, including all critical items, is actively managed and controlled (e.g., a media list maintained, disposal procedures for used media of all types).	All storage media is proactively managed and strictly controlled (e.g., clear owners, unique media serial numbers/tags tracked in an inventory, stored data routinely encrypted).



<i>No IT Security</i>	<i>Basic IT Security</i>	<i>Good IT Security</i>	<i>Excellent IT Security</i>
Uncontrolled data communications with third parties occurs with no restrictions.	Data communications with certain third parties or by certain routes is partially controlled (e.g., network links are secured but not email).	Data communications with most third parties is well controlled, including all critical data and links.	Data communications with third parties is very limited and always strictly controlled, for example, strong authentication and encryption.
Internet/online systems are completely insecure.	Some Internet/online systems and services are partially secured, for example, using commercial EDI/eCommerce services.	Most Internet/online systems and services, including all critical ones, are well secured, for example, using DMZ architecture, managed firewalls, etc.	Internet/online systems and services are very limited and always strictly controlled, for example, digital signatures on all important messages.
No security logging, monitoring, or auditing exists.	Some security logging and monitoring exist, but mostly after the fact, for example, reviewing system, security, audit, or fault logs after incidents.	Routine security logging occurs on most systems with proactive monitoring of all sensitive/critical systems, networks, services, etc.	24/7 security logging and proactive monitoring of all systems, networks, services, etc. is done by dedicated professionals with forensics capability, and system clocks are synchronized to a common atomic reference (cryptographically authenticated).

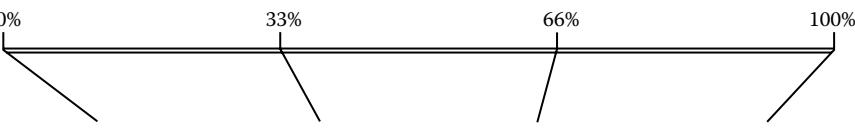
ISO/IEC 27002 Section 11: Information Access Control Maturity Metrics

<i>No Information Access Controls</i>	<i>Basic Information Access Controls</i>	<i>Good Information Access Controls</i>	<i>Excellent Information Access Controls</i>
No access policies or rules of any description exist.	Access policies or rules are partially defined and implemented on some systems (e.g., controlling logical but not physical access) but are generally not well maintained.	Access policies and rules are well defined, implemented, and maintained on most systems, including all sensitive/critical systems, with some compliance activities such as exception logging.	Access policies are formally defined for all systems by information asset owners; rules are proactively implemented, confirmed, maintained, monitored, and periodically reviewed by a dedicated security administration function.



<i>No Information Access Controls</i>	<i>Basic Information Access Controls</i>	<i>Good Information Access Controls</i>	<i>Excellent Information Access Controls</i>
No individual system accounts are in place—everyone shares administrator rights and can use powerful system utilities; there are no passwords or at least no password rules and no awareness or training in this area; users never screen-lock, log off, or clear their desks; it's a free-for-all, and hence, there is no personal accountability.	Basic user registration procedures and controls (e.g., personal user IDs and passwords) for access to some IT systems, services, and utilities are in place; users sometimes screen-lock, log off, or clear their desks; there is a vague attempt at defining password rules plus leaver/de-registration procedures, etc., hence minimal accountability.	User registration and de-registration policies, procedures, and a variety of other controls govern and record access to most information assets with additional controls such as accountable owners, management approval for access, password complexity and reuse rules, security awareness, inactivity timeouts with automatic password locks, and multifactor authentication for all sensitive/critical systems, privileged and shared accounts, with some reviews.	Comprehensive, well-designed, and strictly imposed user identification, authentication, and access controls are in place, including well-written and mandatory policies, procedures, standards, and guidelines plus training and awareness, management authorization for access (especially to privileged accounts and powerful utilities), biometrics and smart cards on lanyards or dog tags where appropriate, personal accountability for all access, routine access logging with monitored alerts, and periodic reviews plus ad hoc unannounced audits.

460 ■ Appendix H



The diagram shows a horizontal scale at the top with four tick marks labeled 0%, 33%, 66%, and 100%. Three vertical lines extend downwards from the 33%, 66%, and 100% marks, each pointing to the middle of the first, second, and third table rows respectively.

<i>No Information Access Controls</i>	<i>Basic Information Access Controls</i>	<i>Good Information Access Controls</i>	<i>Excellent Information Access Controls</i>
No controls exist over network access, no firewalls, no network security monitoring, no idea who might be using the network.	Access controls exist on some networks and access points (e.g., basic firewalls), but they are generally not well managed and have numerous gaps (e.g., insecure wireless LANs, no monitoring, insecure remote access).	Decent access controls exist on most networks and network access points (e.g., professional firewalls), especially on networks containing sensitive/critical systems, and are actively managed with some intrusion detection.	Strong access controls exist on all networks and network access points (e.g., professionally managed firewalls) with proactive 24/7 monitoring and responses, including some automated intrusion prevention.
No access controls exist within applications.	Some access controls exist within some applications, but they are inconsistent and not monitored.	Appropriate authentication and access controls exist within most applications, especially controlling access to powerful system functions and overrides.	Strong identification, authentication, and access controls exist within all applications, controlling access to sensitive or valuable data, powerful system functions, overrides, logs, etc.



<i>No Information Access Controls</i>	<i>Basic Information Access Controls</i>	<i>Good Information Access Controls</i>	<i>Excellent Information Access Controls</i>
Mobile/portable devices and remote access are not secured at all.	Some mobile/portable devices are partially secured, and remote access is partially secured.	Most mobile/portable devices and remote access are secured, especially concerning access to and processing of sensitive or valuable data.	Very few mobile/portable devices exist, and all are strictly controlled with very strong security, including routine encryption and strong authentication for remote access (where permitted).

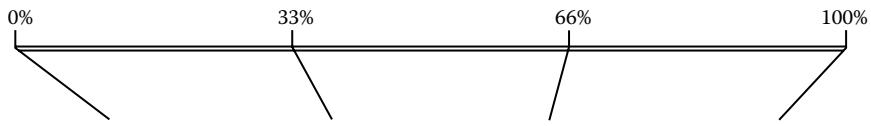
ISO/IEC 27002 Section 12: Software Security Maturity Metrics*



<i>No Software Security</i>	<i>Basic Software Security</i>	<i>Good Software Security</i>	<i>Excellent Software Security</i>
Information security risks and control requirements are not determined for any information systems.	Information security risks and control requirements are determined for some information systems.	Information security risks are analyzed and control requirements determined and documented for most information systems, including all sensitive/critical systems.	Information security risks are analyzed systematically, and control requirements are determined and formally documented for all information systems, for example, using protection profiles.

* ISO/IEC 27001:2005 calls this section “Information systems acquisition, development and maintenance.”

462 ■ Appendix H

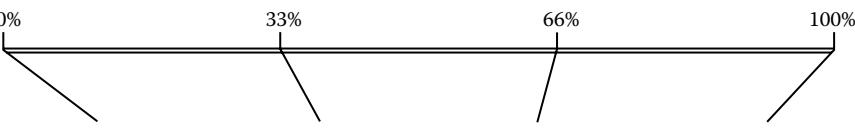


No Software Security	Basic Software Security	Good Software Security	Excellent Software Security
Validation is an alien concept; inaccurate, incomplete, out of date, and malicious data are everywhere.	Validation is incorporated into some processes and systems, but it is quite weak; it is not too hard to force invalid information into, through, or out of processes systems.	Most processes and systems include appropriate validation, especially for the entry of critical data and for all Web-enabled applications.	It is virtually impossible to enter, process, or output invalid data from the processes, systems, and networks because the validation controls and self-checking routines are so strong.
No cryptography exists.	Weak cryptography exists, perhaps using deprecated algorithms (e.g., WEP, DES) or short/weak keys, with no real key management.	Strong cryptography exists in accordance with policy, using current algorithms and key management, protecting most data and all highly sensitive/valuable data.	Military-grade cryptography and strong key generation and management applied as per formal policies and standards with additional controls (such as secure key injectors and duress codes) where appropriate.
Systems are not secured; even vendor-default security configurations are relaxed in practice.	Systems are mostly secured using out-of-the-box vendor defaults.	Most systems, including all sensitive/valuable ones, are secured above the basic default level.	All systems are highly secure, building systematically on a strong security baseline with custom security configurations on many.



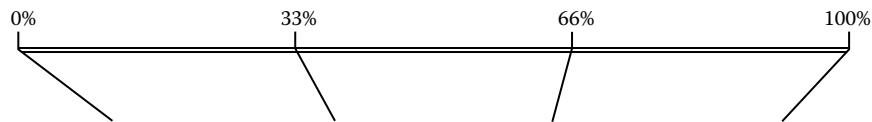
<i>No Software Security</i>	<i>Basic Software Security</i>	<i>Good Software Security</i>	<i>Excellent Software Security</i>
No software development processes exist as such; hence, software security is considered a nonissue.	Software development processes incorporate basic security activities, though compliance is rather hit or miss.	Development processes incorporate risk analysis, security architecture, security testing, etc. with additional controls for highly sensitive/valuable systems.	Rigorous development processes incorporate security activities throughout, including formal security designs and source code security analysis as needed.
Anarchy: frequent data, process, system, and software changes are entirely uncontrolled and unrestricted with management being largely out of the picture, a chaotic mess, the information security manager's worst nightmare.	Some changes are controlled by management albeit somewhat inconsistently (e.g., outsourced developments and commercial software, including patches, implemented without proper security specifications and tests); lots of "emergency" changes with minimal documentation.	Most changes, including <i>all</i> changes to sensitive/valuable systems and processes, are well controlled, for example, security aspects specified in detail, new software and patches security tested prior to implementation, very few emergency changes with decent documentation, neatly filed.	<i>Hardly any</i> changes are permitted; <i>all</i> justified changes are strictly controlled, rigorously assessed, and authorized with a highly formalized change process with copious security documentation, no emergencies.

464 ■ Appendix H



No Software Security	Basic Software Security	Good Software Security	Excellent Software Security
Technical vulnerabilities are unknown; there is no imperative or process to identify them; exploits and incidents come as a complete surprise; black hats rule the roost.	Some technical vulnerabilities are identified and resolved, typically by ad hoc patching some indeterminate time after vendors release security updates.	Most technical vulnerabilities are systematically identified and resolved reasonably promptly, especially on sensitive/critical systems; largely defensive vulnerability assessments include some ad hoc penetration testing by white hats.	Technical vulnerabilities are (almost) completely eliminated through formal design; routine and proactive vulnerability assessment includes penetration testing by competent offensive security professionals (red-teaming).

ISO/IEC 27002 Section 13: Information Security Incident Management Maturity Metrics



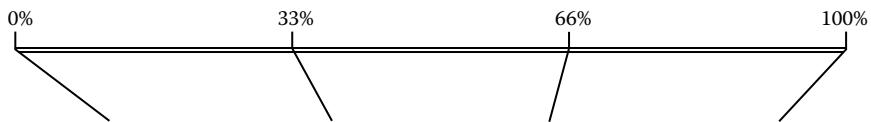
<i>No Information Security Incident Management</i>	<i>Basic Information Security Incident Management</i>	<i>Good Information Security Incident Management</i>	<i>Excellent Information Security Incident Management</i>
No incident management policies, procedures, or guidelines exist to speak of.	Some incident management policies, procedures, and guidelines are in place, but they are of dubious quality and incomplete coverage.	A set of incident management policies, procedures, and guidelines is in place, covering at least the key IMT activities.	A comprehensive suite of incident management policies, procedures, etc. is in place, properly authorized or mandated by management, of good quality and proactively maintained.
Incidents are not reported—most aren't even recognized in fact.	Some incidents are reported; incident awareness/training activities take place, but they are relatively unstructured and sporadic or reactive in nature; compliance is low; incident handling is hit or miss, a low priority.	The security awareness and training program encourages everyone to report incidents and near misses, etc. promptly to a single focal point according to policy; compliance is good; most incidents are quite well handled on the whole.	Events, incidents, near misses, vulnerabilities, etc. are always reported promptly and accurately and are handled professionally, systematically, and efficiently as a matter of urgency.

466 ■ Appendix H



The diagram shows a horizontal scale with arrows pointing downwards from the numbers 0%, 33%, 66%, and 100% towards the table below.

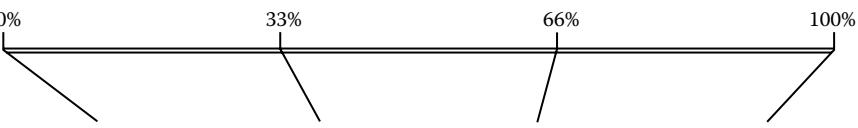
<i>No Information Security Incident Management</i>	<i>Basic Information Security Incident Management</i>	<i>Good Information Security Incident Management</i>	<i>Excellent Information Security Incident Management</i>
There is no incident management team (IMT) of any description: information security incidents are neither managed nor resolved.	There is a small and immature IMT, possibly just a few nominees and part-timers who may not have the background experience to appreciate their responsibilities, or it is outsourced to the cheapest bidder who deals with everything.	The IMT is composed of a few competent, trained individuals, or it is outsourced to a competent specialist outfit that maintains close ties to the organization; scheduled tests and exercises (rehearsals) take place occasionally.	The IMT is a dedicated and competent professional unit with the necessary forensic skills, expertise, structure, management support, authority, policies, procedures, etc.; rehearsals are frequent and sometimes unannounced.
"Post incident reviews [PIRs]: what are they—something to do with intruder detectors maybe?"	PIRs may take place after selected incidents, but they are not necessarily formalized or well structured, and the outcomes are sometimes hard to fathom (actual security improvements are quite rare).	PIRs are conducted for all major internal incidents and significant third-party incidents or near misses; the process is standardized, for example, a fixed agenda and reporting format with suitable participants being invited; security improvements generally follow as a rule.	PIRs for all major incidents and near misses (including some affecting third parties) are formalized and structured appropriately; security improvements happen systematically resulting from rigorous root cause analysis and agreed-upon action plans that actually get done on time.

ISO/IEC 27002 Section 14: Business Continuity Management Maturity Metrics*


<i>No Business Continuity Management</i>	<i>Basic Business Continuity Management</i>	<i>Good Business Continuity Management</i>	<i>Excellent Business Continuity Management</i>
Nothing even vaguely approximating a policy toward business continuity is in place.	Something vaguely approximating a policy toward business continuity is in place though it's not very well documented, hard to locate, and probably out of date.	A clear strategy toward business continuity is supported by a firm policy owned and authorized by management and actively maintained.	A coherent and comprehensive business continuity strategy is supported by suitable policies, procedures, guidelines, and practices with strong coordination with other relevant parties.
Business continuity requirements are completely unknown.	Major business continuity requirements are identified but typically just those mandated on the organization by law with limited documentation.	Business impact analysis is used systematically from time to time to identify, characterize, and document business continuity requirements, both internal and external.	Business continuity requirements are thoroughly analyzed, documented, and constantly maintained through business impact analysis, compliance assessments, business analysis, disaster analysis, etc.

* This section deliberately goes beyond the rather basic approach in ISO/IEC 27002:2005.

468 ■ Appendix H



The diagram shows a horizontal scale with arrows pointing downwards from the numbers 0%, 33%, 66%, and 100%. The scale is positioned above a table.

<i>No Business Continuity Management</i>	<i>Basic Business Continuity Management</i>	<i>Good Business Continuity Management</i>	<i>Excellent Business Continuity Management</i>
No resilience: the organization is extremely fragile and will collapse in a heap at the first hint of trouble.	Some resilience: the organization can probably resist minor incidents, but disasters are likely to prove disastrous.	Strong resilience: the core business processes should continue operating despite most incidents but may be affected a little by disasters (e.g., noticeably worse performance).	Excellent resilience: most business processes including all the critical ones will definitely continue unaffected despite practically any incident or disaster.
No recovery capability: following a disaster, everything will need to be rebuilt from scratch, assuming there is anyone left who can do it without any documentation.	Some disaster recovery capability: certain IT systems may be recovered from backups provided suitable equipment can be found; there is some documentation, though it's often incomplete and out of date.	Strong recovery capability: most IT systems and business processes, including all the essential ones, can be recovered from backups on standby equipment or using alternative sources, following documented procedures.	Excellent disaster recovery and business resumption capability with facilities, equipment, backups, supplies, people, etc. readily available to recover from almost any eventuality, following documented and well-rehearsed procedures.



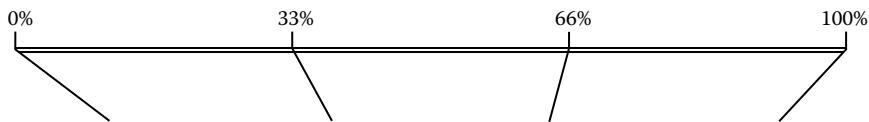
<i>No Business Continuity Management</i>	<i>Basic Business Continuity Management</i>	<i>Good Business Continuity Management</i>	<i>Excellent Business Continuity Management</i>
"Contingency: what's that?" Management naïvely assumes that it will somehow muddle through or rely on the authorities; staff expects to be out of a job.	Basic emergency/crisis planning exists with something written down somewhere; there are minimal essential supplies (e.g., first aid kits) and possibly unrealistic expectations of help from authorities, partners, suppliers, and customers.	Good contingency planning and documented arrangements are largely self-contained with sensible emergency supplies on hand and a preordained contingency or disaster management structure, including an invocation or call-out process and procedures and training for key managers/team leaders at least.	Excellent contingency arrangements, including copious emergency supplies, resilient people, facilities, communications, etc., operate within a well-thought-out contingency/crisis/disaster management structure; excellent training and development fosters a genuine can-do, cope-with-anything, survivalist attitude; thorough exercises and simulations involve business partners.

470 ■ Appendix H



A horizontal scale at the top of the table shows percentages: 0%, 33%, 66%, and 100%. Three vertical lines extend downwards from these percentage points, each pointing to one of the four rows in the table below.

<i>No Business Continuity Management</i>	<i>Basic Business Continuity Management</i>	<i>Good Business Continuity Management</i>	<i>Excellent Business Continuity Management</i>
No continuity arrangements exist to test, hence no demand for assurance.	Minimal business continuity tests (e.g., desk-based reviews on certain parts) are conducted sporadically; actions arising are mostly left to chance resulting in low assurance.	Advanced continuity tests against predefined test objectives are done plus regular exercises and rehearsals; findings are captured in action plans for improvements that are assigned to responsible individuals, checked, and signed off on completion; good assurance.	Business continuity arrangements are thoroughly tested and proven against detailed specifications, including independent confirmation; frequent exercises and rehearsals are done, some full-scope plus live-fire, peak-time disaster simulations implying very high assurance and confidence in the arrangements.

ISO/IEC 27002 Section 15: Information Security Compliance Management Maturity Metrics*


<i>No Information Security Compliance</i>	<i>Basic Information Security Compliance</i>	<i>Good Information Security Compliance</i>	<i>Excellent Information Security Compliance</i>
There is no pressure to comply with externally imposed information security obligations; no process is in place even to identify potentially applicable requirements; compliance failures and penalties are a foregone conclusion; there are no corporate lawyers.	There is some pressure to comply with certain externally imposed information security obligations and basic mechanisms to identify and assess the requirements; compliance status is checked in an ad hoc fashion; compliance failures are distinctly possible; the lawyers take the lead on compliance matters.	There is strong pressure to comply with all applicable externally imposed information security obligations; requirements are systematically identified, analyzed, and addressed; compliance status is routinely assessed; compliance failures are unlikely; lawyers and risk and security people collaborate on compliance.	Most security practices far exceed minimal compliance obligations; hence, noncompliance is barely a remote possibility; nevertheless, processes are in place to identify requirements and confirm compliance systematically with independent confirmation where justified; compliance professionals take the lead.

* ISO/IEC 27002:2005 refers to information security obligations imposed by laws concerning intellectual property rights, protection of business records, privacy, computer misuse, and cryptography. We deliberately avoid being so specific because laws and regulations vary markedly around the globe, and that list is incomplete.

472 ■ Appendix H



The diagram shows a horizontal scale at the top with four tick marks labeled 0%, 33%, 66%, and 100%. Three vertical lines extend downwards from the 33%, 66%, and 100% marks, each pointing to the start of one of the four rows in the table below.

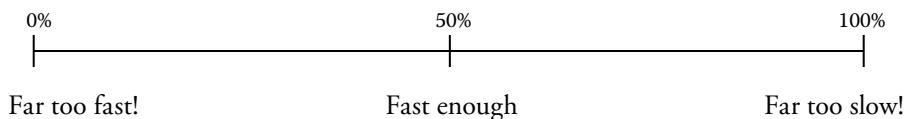
<i>No Information Security Compliance</i>	<i>Basic Information Security Compliance</i>	<i>Good Information Security Compliance</i>	<i>Excellent Information Security Compliance</i>
Few, if any, information security policies, standards, procedures, etc. exist; hence, compliance is moot; no internal compliance checks or related practices take place; third-party compliance with the organization's requirements (e.g., to protect its intellectual property) is not even considered because such requirements are seldom specified anyway.	Some checks and other activities take place to drive up compliance with certain security policies, etc., but they are inconsistently applied, and compliance is distinctly variable in practice; disciplinary procedures are weak and ineffective; some security requirements are mandated on third parties, but compliance is barely considered.	Compliance with most internally derived and mandated security requirements, including all the important ones, is achieved by a sound system of awareness and training, compliance checking (including technical reviews), improvement, and enforcement activities, including disciplinary action; third-party compliance with obligations contractually imposed by the organization is sometimes confirmed by discussion or by inspection while compliance with ISO27k etc. is recommended for some suppliers and business partners.	Requirements specified in security policies, procedures, etc. and mandated by management are routinely accompanied by compliance activities; a very strong compliance culture, reinforced by harsh penalties, including prosecution, means noncompliance is readily identified and extremely rare; third-party compliance is routinely confirmed by inspections and audits, and harsh penalties are imposed there, too; suppliers and business partners are required to be certified compliant with ISO/IEC 27001 or similar standards.



Free ebooks ==> www.ebook777.com

Appendix I: Sample Management Survey

How fast would you personally say your part of the organization is changing? Please mark the following scale at the appropriate point, in your opinion:



What led you to give that score? Are there any specific incidents or situations that particularly concern you? Have you anything else to add? Feel free to comment in the box below.

Please return the completed form to the information security manager via the internal mail. All responses received by [date] will be entered into a prize drawing. You are welcome to remain anonymous, but if you wish to participate in the drawing, please tell us your name:

Free ebooks ==> www.ebook777.com

Appendix J: Observer Bias

The alert information security manager needs to be aware of his or her own cognitive biases, plus those of the intended audiences or consumers of the metrics and, potentially, even the people making the base measurements. It's important to keep in mind that numerous studies have shown we humans are notoriously poor at estimating risk and acting appropriately even when we have objective factual information and ample warning. Anyone for a smoke?

Studies typically show that risk is gauged and acted upon more often as a result of instinctive gut reaction than by a reasoned or rational process. For example, one shark attack clears the beaches across the country even though one is far more likely (43 times more!) to be killed by a lightning strike on a golf course. These reactions are further shaded by a host of evolutionary and environmental biases that render it virtually certain we'll mostly get it wrong. The point is that understanding and awareness can, at least, serve to compensate and reduce the margin of error.

A particular form of bias (one of more than 40 recognized biases) is called *biased assimilation*. This is the normal human tendency to pay attention only to those facts that support our personal agenda while discarding or disregarding those that don't. We see this all the time in politics: politicians on TV gladly discuss and do their best to focus the audience's attention on socioeconomic indicators that reflect positively on them and negatively on the opposition while doing their best to ignore or downplay others. Outside the media circus, observer bias is a deeper issue if the politicians and civil servants literally disregard metrics that are unfavorable or indicate issues that are difficult to tackle. Observer bias can even affect the choice of metrics, making it an insidious threat to the process of developing a system of metrics.

The status quo bias is about favoring the familiar over something novel or different even when it's demonstrably not working. It's the old saw about continuing to do the same thing that has failed repeatedly and expecting a different result.

A number of other biases shown by researchers in behavioral economics affect how decisions are made. Having some familiarity with these normal tendencies can help counteract effects resulting in bad decisions.

The following list (Kahneman et al. 1982) is not meant to be comprehensive but may be relevant to information security decisions based on interpretation of metrics. That is to say, information, even if accurate, is subject to all sorts of biases in the interpretation and subsequent decisions based on it. Some of the more common include the following:

- *Attentional bias*: the tendency to neglect relevant data when making judgments of a correlation or association. For instance, we may place more emphasis on security threats that are frequently in the news headlines (such as hackers) while disregarding others (such as typos and other human errors) that are, in fact, more numerous or more dangerous but less newsworthy.
- *Choice-supportive bias*: the tendency to remember one's choices as better than they actually were. Having dubiously picked a technology, product, or vendor that ends up becoming the market leader, we are unlikely to recall or mention our doubts at the time.
- *Confirmation bias*: the tendency to search for or interpret information in a way that confirms one's preconceptions. If we strongly believe Apple products are much less prone to malware, we may discount or dismiss reports to the contrary, assuming we even bother to read them.
- *Congruence bias*: the tendency to test specific hypotheses exclusively through direct testing as opposed to a more open approach that considers and tests possible alternative hypotheses as well.
- *Distinction bias*: the tendency to view two options as more dissimilar when evaluating them simultaneously than when evaluating them separately. This sometimes leads to the situation known as a false dichotomy, where we put ourselves in the position of choosing between options as alternatives when, in fact, both may be valid.
- *Egocentric bias*: when people claim more responsibility for themselves for the results of a joint action than an outside observer would. A successful information security management system does not solely reflect the drive and work of the information security manager, or the information security department: it draws on a wide range of people and functions, extending to most if not all employees (staff and management) and usually third parties, such as consultants and business partners.
- *Forward bias*: the tendency to create models based on past data that are validated only against those past data. This may be the source of the phrase "That's the way we've always done it."
- *Hindsight bias*: sometimes called the I-knew-it-all-along effect, the tendency to see past events as being predictable at the time those events happened. Having ignored or neglected certain information security risks and survived

without incident, we may subsequently rationalize it, believing or even claiming that we wisely made a definite risk acceptance decision. Conversely, if an incident occurs, we may say, “See, I told you it would happen!,” whereas it was never so clear.

- *Normalcy bias:* the refusal to plan for, or react to, a disaster that has never happened before. This is a huge issue in relation to business continuity planning. Imagine how difficult it must have been, prior to 9/11, to plan for the possibility of total physical destruction of one of the twin towers, let alone both. Truly extreme risks that exceed even our worst-case-scenario thinking often remain largely or completely untreated.
- *Omission bias:* the tendency to judge harmful actions as worse or less moral than equally harmful omissions (inactions). Failing to lock a ground-floor office window before leaving the office (according to clear security procedures and responsibilities) is just as bad as the intrusion and office theft that results.
- *Optimism bias:* the tendency to be overly optimistic about the outcome of planned actions. We tend to assume our security controls work more reliably than they do. Procedural or manual security controls are a classic example: no matter how well documented and regardless of the amount of training, people will occasionally take insecure shortcuts through expediency, neglect, carelessness, or forgetfulness. Robust fail-safe controls aim to take this into account (and even that they are fail-safe is an assumption worth checking!).
- *Outcome bias:* the tendency to judge a decision by its eventual outcome instead of based on the quality of the decision at the time it was made. We may be so relieved that a control implementation project finally succeeds after a lot of additional, unplanned effort that we forget we could have chosen other approaches, which, as it turns out, might have been cheaper and easier.
- *Overconfidence effect:* excessive confidence in one’s own answers to questions. Information security is largely a matter of risk management, and risk is all about uncertainty. However much we attempt to bring everything under control, things can and will go wrong, but if we are not prepared for that, we can be caught seriously off guard and unprepared or unable to handle the incidents.
- *Pessimism bias:* the tendency for some people, especially those suffering from depression, to overestimate the likelihood of negative things happening to them. Many information security and risk management professionals are naturally risk-averse, and almost all are *perceived* that way by other business people.
- *Positive outcome bias:* the tendency of one to overestimate the probability of a favorable outcome coming to pass in a given situation. In New Zealand, we say, “She’ll be right,” as in “Don’t worry, it will work out alright in the end.” We do our level best to recall things that went well while trying not to dwell on our mistakes, which skews our perception of the probabilities of certain types of security incidents.

480 ■ Appendix J

- *Projection bias*: the tendency to unconsciously assume that others (or one's future selves) share one's current emotional states, thoughts, and values. A moralistic, strongly ethical person may be astounded to discover that he or she has been taken for a ride by a fraudster.
- *Selective perception*: the tendency for expectations to affect perception. Things may seem better or worse than they really are if we thought they would be better or worse, respectively.
- *Self-serving bias*: the tendency to claim more responsibility for successes than failures or the tendency for people to evaluate ambiguous information in a way beneficial to their interests.
- *Semmelweis reflex*: the tendency to reject new evidence that contradicts an established paradigm. Novel information security attacks often exploit long-standing security vulnerabilities, catching victims unaware and incredulous even when the flaws are patently being exploited. Denial is often the first stage of the response.
- *Social comparison bias*: the tendency, when making hiring decisions, to favor potential candidates who don't compete with one's own particular strengths. Could also be termed the sycophancy bias—a tendency for powerful figures to be surrounded by yes men and to actively avoid criticisms or alternative approaches suggested by those with different mindsets (such as auditors).
- *Zero-risk bias*: preference for reducing a small risk to zero over a greater reduction in a larger risk. This is an interesting one! Spend a thousand dollars either to *eliminate* the chances of aliens taking over the computer suite or to slightly, almost imperceptibly reduce the number of security-related bugs in our software? You choose!

Because perception and interpretation vary to such a great extent, it is important from a credibility standpoint to compensate responses to information, events, and metrics through an awareness of these biases—or perhaps, if you want to be more proactive about it, to point out or even exploit these biases in how you position, present, and discuss security matters. The biases affect those designing, producing, and consuming security metrics.

Appendix K: Observer Calibration

Appendix J raises the thorny issue of how to deal with observer biases in such a way that they don't derail efforts to arrive at reasonably objective, reliable, and repeatable answers. Certainly, being aware of them can help. Most of us can identify some of the tendencies and susceptibilities within us. But often we need to do more.

One possible solution comes from Hubbard (2010) in the form of training or "calibrating" observers to gauge probabilities more objectively, counteracting their tendency to be either underconfident or overconfident. Hubbard suggests trainees should practice on a series of trivial questions, providing feedback to each other to fine-tune their ability to assess probabilities. This is obviously relevant when considering the probability of information security incidents or interpreting the result of some metric and deals with the issue of uncertainty.

Research by Hubbard and others has shown that experts tend to be overconfident with their ability to determine probabilities. Because they may be either providing the crucial metrics on which managers base vital decisions or, at least, strongly influencing those decisions, the experts are gambling with their own credibility.

Calibration is also worthwhile in situations where teams of observers, assessors, or auditors are independently measuring relatively subjective factors in different parts of a large organization or in separate organizations. Assuming the entire team is supposed to be applying the same criteria (e.g., all using the same maturity metric scales described in Appendix H), calibration can be achieved as follows:

1. First, the team assembles for training on the assessment method with plenty of time to discuss and agree on the objectives, the process, and the scoring criteria.
2. Next, junior team members are paired up with their more experienced colleagues to undertake one or more initial assessments together, discussing and, if appropriate, adjusting the scores and learning as they go.

482 ■ Appendix K

3. The bulk of the assessments can be performed by the assessors working alone, utilizing their training and the documented criteria to the best of their abilities and keeping notes on any issues or doubts.
4. Finally, the team reassembles to discuss, consider, and, where necessary, normalize the scores prior to preparing the metricated report.

Appendix L: Bibliography

Aside from providing sufficient information for you to locate reference sources specifically cited in the text, we recommend the following resources for further reading on this topic.

- Accenture (2009). *How Global Organizations Approach the Challenge of Protecting Personal Data*. Survey conducted in 2008 by Ponemon Institute. www.accenture.com/SiteCollectionDocuments/PDF/Accenture_DPP_Report_FINAL.pdf.
- Barabanova, Rostyslav (2011). *Information Security Metrics: State of the Art*. DSV Report series no. 11-007.
- Berinato, Scott (2005). "A few good information security metrics." *CSO Magazine*. www.csionline.com/article/220462/a-few-good-information-security-metrics.
- Brenot, Jean, Bonnefous, Sylviane, and Marris, Claire (1998). "Testing the cultural theory of risk in France." *Risk Analysis* 18, no. 6.
- Brotby, Krag (2009a). *Information Security Management Metrics*. CRC Press, Boca Raton, FL.
- Brotby, Krag (2009b). *Information Security Governance: A Practical Development and Implementation Approach*. Wiley, New Jersey.
- Cameron, Kim, and Quinn, Robert (1999). *Diagnosing and Changing Organizational Culture*. Addison-Wesley, New Jersey.
- Campbell, George K. (2006). *Measures and Metrics in Corporate Security: Communicating Business Value*. The Security Executive Council, Marietta, GA.
- CIS (2010). *CIS Consensus Security Metrics*. Center for Internet Security. benchmarks.cisecurity.org/en-us/?route=downloads/browse/category.metrics.
- Deloitte (2010). "The final act: Financial reporting implications of the Dodd–Frank Wall Street Reform and Consumer Protection Act." *Heads Up* 17, no. 26.
- GAO (1998). *Measuring Performance and Demonstrating Results of Information Technology Investments*. United States General Accounting Office, Accounting and Information Management Division. Executive Guide. www.gao.gov/assets/80/76378.pdf.
- Gordon, Lawrence A., and Loeb, Martin P. (2006). *Managing Cyber-security Resources: A Cost-Benefit Analysis*. McGraw-Hill, New York.
- Hauser, John R., and Katz, Gerald M. (1998). *Metrics: You Are What You Measure*. [www.mit.edu/~hauser/Papers/Hauser-Katz Measure 04-98.pdf](http://www.mit.edu/~hauser/Papers/Hauser-Katz%20Measure%2004-98.pdf).
- Hayden, Lance (2010). *IT Security Metrics: A Practical Framework for Measuring Security and Protecting Data*. McGraw-Hill Osborne Media, New York.

484 ■ Appendix L

- Herrmann, Debra S. (2007). *Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience and ROI*. Auerbach Publications, Boca Raton, FL.
- Hinson, Gary (2006). "Seven Myths About Security Metrics." *ISSA Journal*, July.
- Hubbard, Douglas (2010). *How to Measure Anything: Finding the Value of Intangibles in Business*, Second edition. Wiley, New Jersey.
- ISACA (2009). *An Introduction to the Business Model for Information Security*. ISACA.
- ISACA (2010). *Return on Security Investment*. IT Audit and Assurance Guideline G41. www.isaca.org/Knowledge-Center/Standards/Documents/G41-ROSI-5Feb10.pdf.
- ISACA (2011). *COBIT*. ISACA.*
- ISACA (2012). *Certified Information Security Manager Review Manual 2012*. ISACA.
- ISO/IEC 27001 (2005). *Information Technology—Security Techniques—Specification for an Information Security Management System*. International Organization for Standardisation/International Electrotechnical Committee. Republished by many national standards bodies.
- ISO/IEC 27002 (2005). *Information Technology—Security Techniques—Code of Practice for Information Security Management*. International Organization for Standardisation/International Electrotechnical Committee. Republished by many national standards bodies.
- ISO/IEC 27004 (2009). *Information Technology—Security Techniques—Information Security Management—Measurement*. International Organization for Standardisation/International Electrotechnical Committee. Republished by many national standards bodies.
- ITGI (2005). *Information Security Governance: Guidance for Boards of Directors and Executive Management*. IT Governance Institute.
- ITGI (2006). *Information Security Governance: Guidance for Boards of Directors and Executive Management*, Second edition. IT Governance Institute.
- ITGI (2008a). *Val IT Framework 2.0.*† www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Val-IT-Framework-2.0.aspx.
- ITGI (2008b). *Information Security Governance: Guidance for Information Security Managers*. IT Governance Institute.
- Jaquith, Andrew (2007). *Security Metrics: Replacing Fear, Uncertainty, and Doubt*. Addison-Wesley, New Jersey.
- Kahneman, D., Slovic, P., and Tversky, A. (1982). *Judgment Under Uncertainty: Heuristics and Biases*. Cambridge University Press, New York.
- Kaplan, Robert S., and Norton, David P. (1996). *The Balanced Scorecard: Translating Strategy into Action*. Harvard Business School Press. Builds on their groundbreaking article in the *Harvard Business Review*, Jan.–Feb. 1992.
- Kiely, Laree, and Benzel, Terry (2006). "Systemic security management. Security & privacy." *IEEE* 4, no. 6: 74–77.
- Machiavelli, Nicolo (unpublished).‡ *The Prince*. A translation by W. K. Marriott in 2006 is available in its entirety at www.gutenberg.org/files/1232/1232-h/1232-h.htm.

* While at the time of writing COBIT 4.1 was the current release, COBIT 5 has since been released.

† COBIT 5 integrates Val IT, Risk IT, and BMIS into COBIT.

‡ Although the original work was not published in Machiavelli's lifetime (1469–1527), it was plagiarized and circulated.

- Mayer, John D., Salovey, Peter, Caruso, David R., and Sitarenios, Gill (2003). "Measuring emotional intelligence with the MSCEIT V2.0." *Emotion* 3: 97–105.
- McGraw, Gary (2006). *Software Security: Building Security In*. Addison-Wesley, New Jersey.
- Myers, Isabel Briggs, McCaulley, Mary H., Quenk, Naomi, and Hammer, Allen (1998). *MBTI Manual: A Guide to the Development and Use of the Myers-Briggs Type Indicator*. Third edition. Consulting Psychologists Press, Palo Alto, CA.
- NIST SP 800-55 (2008). *Performance Measurement Guide for Information Security*. NIST Special Publication.*
- OCEG (2006). *Measurement & Metrics Guide: Performance Measurement Approach and Metrics for a Compliance and Ethics Program*. Practice guide. Open Compliance & Ethics Group. www.OCEG.org.
- Olsina, Luis, and Rossi, Gustavo (2002). "Measuring Web application quality with WebQEM." *IEEE Multimedia* 9, no. 4: 20–29.
- OSVDB (online). Open Source Vulnerability Database. <http://osvdb.org>.
- Paulk, Mark C., Weber, Charles V., Curtis, Bill, and Chrissis, Mary Beth (1995). *The Capability Maturity Model: Guidelines for Improving the Software Process*. Addison Wesley, New Jersey.
- PwC (2011). *2012 Global State of Information Security Survey*. 14th annual survey. www.pwc.com/gx/en/information-security-survey.
- SABSA (online) Sherwood Applied Business Security Architecture. www.SABSA.org.
- Stefani, Antonia, and Xenos, Michalis (2009). "Meta-metric evaluation of ECommerce-related metrics." *Electronic Notes in Theoretical Computer Science* 233: 59–72.
- Stoll, Clifford (1989). *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. Bodley Head, Doubleday, New York.
- Taleb, Nassim N. (2010). *The Black Swan: The Impact of the Highly Improbable*. Second edition. Random House, New York.
- Thorp, John (1998). *The Information Paradox: Realizing the Business Benefits of Information Technology*. McGraw-Hill, Toronto. [DMR's Center for Strategic Leadership is also credited.]
- Wong, Caroline (2012). *Security Metrics: A Beginner's Guide*. McGraw-Hill, New York.
- www.SecurityMetametrics.com. Companion Web site for this book with additional materials to download, a catalog of PRAGMATIC metrics, and a forum to participate in the discussion.

* The 2008 revision 1 of SP 800-55 is substantially better than the original version. Our book *may* hit the streets too late in the day to influence revision 2, but we sincerely hope the NIST team working on SP 800-55 find something of value in the PRAGMATIC approach for revision 3.

Free ebooks ==> www.ebook777.com

Other books on information security metrics discuss number theory and statistics in academic terms. Light on mathematics and heavy on utility, **PRAGMATIC Security Metrics: Applying Metametrics to Information Security** breaks the mold. This is the ultimate how-to-do-it guide for security metrics.

Packed with time-saving tips, the book offers easy-to-follow guidance for those struggling with security metrics. Step by step, it clearly explains how to specify, develop, use, and maintain an *information security measurement system* (a comprehensive suite of metrics) to help:

- Security professionals systematically improve information security, demonstrate the value they are adding, and gain management support for the things that need to be done
- Management address previously unsolvable problems rationally, making critical decisions such as resource allocation and prioritization of security relative to other business activities
- Stakeholders, both within and outside the organization, be assured that information security is being competently managed.

The PRAGMATIC approach lets you hone in on your problem areas and identify the few metrics that will generate real business value. The book:

- Helps you figure out exactly *what* needs to be measured, *how* to measure it, and most importantly, *why* it needs to be measured
- Scores and ranks more than 150 candidate security metrics to demonstrate the value of the PRAGMATIC method
- Highlights security metrics that are widely used and recommended, yet turn out to be rather poor in practice
- Describes innovative and flexible measurement approaches such as capability maturity metrics with continuous scales
- Explains how to minimize both measurement and security risks using complementary metrics for greater assurance in critical areas such as governance and compliance

In addition to its obvious utility in the information security realm, the PRAGMATIC approach, introduced for the first time in this book, has broader application across diverse fields of management including finance, human resources, engineering, and production—in fact any area that suffers a surplus of data but a deficit of useful information.

View the authors' website and blog at: www.securitymetametrics.com



CRC Press

Taylor & Francis Group
an informa business
www.crcpress.com

6000 Broken Sound Parkway, NW
Suite 300, Boca Raton, FL 33487
711 Third Avenue
New York, NY 10017
2 Park Square, Milton Park
Abingdon, Oxon OX14 4RN, UK

K13838

ISBN: 978-1-4398-8152-1



www.auerbach-publications.com

www.ebook777.com