"To paraphrase Lord Kelvin's famous quote, 'You cannot improve what you cannot measure.' Computer security has inhabited this sorry state for years, leaving too much room for snake oil, scare tactics, and plain old bull feathers. Andy's book helps to remedy this problem by sending a strong clear message that metrics are both necessary and possible. Buy this strikingly well-written book today and help put an end to security nonsense."

—**Gary McGraw, Ph.D.,** CTO, Cigital, Author of *Software Security: Building Security In*

SECURITY METRICS

Replacing Fear, Uncertainty, and Doubt

ANDREW JAQUITH

FOREWORD BY DANIEL E. GEER, JR.

Praise for *Security Metrics*

"Throw out the security religion and make informed business decisions now!"

—Mark Curphey
ISBPM, Inc.
"Connecting People, Process and Technology"

"I'm very excited that Jaquith has written a text on metrics, and expect this will be the standard reference for years to come."

—Adam Shostack

"Andrew devotes an innumerable amount of time and effort to helping our profession out at SecurityMetrics.org. His book is wonderful, entertaining, and well thought-out. I found myself nodding my head in agreement more than a few times."

—Alex Hutton
CEO, Risk Management Insight

"Andrew has written a book that most people who work in information protection and those who manage and work with them should read, not because it is particularly informative about information protection, but because it is highly informative about the challenges of measuring protection programs effectively. While lots of books are out there about this or that aspect of security, from a security management standpoint, you cannot manage what you cannot measure, and Andrew puts his stake in the ground with this book about what you should measure and how to do it."

—Dr. Fred Cohen
CEO, Fred Cohen & Associates
http://all.net/

"To paraphrase Lord Kelvin's famous quote, 'You cannot improve what you cannot measure.' Computer security has inhabited this sorry state for years, leaving too much room for snake oil, scare tactics, and plain old bull feathers. Andy's book helps to remedy this problem by sending a strong clear message that metrics are both necessary and possible. Buy this strikingly well-written book today and help put an end to security nonsense."

—Gary McGraw, Ph.D.
CTO, Cigital
Author of *Software Security: Building Security In*

Security Metrics

Table of Contents

Contents

Foreword

Preface

Acknowledgments

About the Author

Chapter 1 Introduction: Escaping the Hamster Wheel of Pain

- Risk Management Is Where the Confusion Is
- Metrics Supplant Risk Management
- Summary

Chapter 2 Defining Security Metrics

- Security Measurement Business Drivers
  - Roadblocks to Data Sharing
- Modeling Security Metrics
  - Modelers Versus Measurers
  - Quality Assurance Literature
  - Public Health Terminology and Reporting Structure
  - Portfolio Management
  - Accelerated Failure Testing
  - Insurance
- What Makes a Good Metric?
  - Metric Defined
  - Consistently Measured
  - Cheap to Gather

Table of Contents

Expressed as a Number or Percentage
Expressed Using at Least One Unit of Measure
Contextually Specific
What Makes a Bad Metric?
Inconsistently Measured
Cannot Be Gathered Cheaply
Does Not Express Results with Cardinal Numbers and Units of Measure
What Are Not Metrics?
Misuse of Security Taxonomies
Annualized Loss Expectancy
Summary
Chapter 3 Diagnosing Problems and Measuring Technical Security
Using Metrics to Diagnose Problems: A Case Study
Defining Diagnostic Metrics
Perimeter Security and Threats
E-mail
Antivirus and Antispam
Firewall and Network Perimeter
Attacks
Coverage and Control
Antivirus and Antispyware
Patch Management
Host Configuration
Vulnerability Management
Availability and Reliability
Uptime
System Recovery
Change Control

Table of Contents

Application Security

Black-Box Defect Metrics

Qualitative Process Metrics and Indices

Code Security Metrics

Summary

Chapter 4 Measuring Program Effectiveness

Using COBIT, ITIL, and Security Frameworks

Frameworks

Not Useful: Asset Valuation

Planning and Organization

Assessing Risk

Human Resources

Managing Investments

Acquisition and Implementation

Identifying Solutions

Installing and Accrediting Solutions

Developing and Maintaining Procedures

Delivery and Support

Educating and Training Users

Ensuring System Security

Identifying and Allocating Costs

Managing Data

Managing Third-Party Services

Monitoring

Monitoring the Process

Monitoring and Evaluating Internal Controls

Ensuring Regulatory Compliance

Summary

Chapter 5 Analysis Techniques

Pearson

Table of Contents

Mean (Average)

Median

Standard Deviation

Grouping and Aggregation

Records and Attributes

Grouping

Aggregation

Time Series Analysis

Cross-Sectional Analysis

Quartile Analysis

Quartile Summary Statistics

First-Versus-Fourth Analyses

Correlation Matrices

Summary

Chapter 6 Visualization

Design Principles

It Is About the Data, Not the Design

Just Say No to Three-Dimensional Graphics and Cutesy Chart Junk

Dont Go off to Meet the Wizard

Erase, Erase, Erase

Reconsider Technicolor

Label Honestly and Without Contortions

Example

Stacked Bar Charts

Waterfall Charts

Time Series Charts

Basic Time Series Charts

Indexed Time Series Charts

Table of Contents

Quartile Time Series Charts

Bivariate (X-Y) Charts

Two-Period Bivariate Charts

Small Multiples

Quartile-Plot Small Multiples

Two-by-Two Matrices

Period-Share Chart

Pareto Charts

Tables

Treemaps

Creating Treemaps

Thinking Like a Cannibal: the Case for Redrawing

A Patch Job for Ecora

Reorienting SecurCompass

Managing Threats to Readability

Summary

Chapter 7 Automating Metrics Calculations

Automation Benefits

Accuracy

Repeatability

Increased Measurement Frequency

Reliability

Transparency

Auditability

Can We Use (Insert Your Favorite Tool Here) to Automate Metrics?

Spreadsheets

Business Intelligence Tools

Table of Contents

Security Event and Incident Management (SIEM) Products

Technical Requirements for Automation Software

Data Model

Threats

Exposures

Countermeasures

Assets

Data Sources and Sinks

Data Sources

Data Sinks

Data Interfaces

Data Source Interfaces

Data Sink (Presentation) Interfaces

Metrics Program Management

Implementing Metrics Automation: a Case Study

Summary

Chapter 8 Designing Security Scorecards

The Elements of Scorecard Style

Complete

Concise

Clear

Relevant

Transparent

The Balanced Scorecard

History

Composition

Flexibility of the Balanced Scorecard

Challenges and Benefits of the Balanced Scorecard

Creating the Balanced Security Scorecard

Table of Contents

The Case Against Security-Centric Balanced Scorecards

The Process of Creating the Balanced Security Scorecard

Financial Perspective

Customer Perspective

Internal Process Perspective

Learning and Growth Perspective

Organizational Considerations for the Balanced Security Scorecard

Cascading Scorecards Build Bridges

Balancing Accountability and Acceptance

Speeding Acceptance Using Mock-Ups

Summary

Index

Pearson