

Security Metrics: Replacing Fear, Uncertainty, and Doubt

By Andrew Jaquith

Download Read Online

Security Metrics: Replacing Fear, Uncertainty, and Doubt By Andrew Jaquith

<>**The Definitive Guide to Quantifying, Classifying, and Measuring Enterprise IT Security Operations**

Security Metrics is the first comprehensive best-practice guide to defining, creating, and utilizing security metrics in the enterprise.

Using sample charts, graphics, case studies, and war stories, Yankee Group Security Expert Andrew Jaquith demonstrates exactly how to establish effective metrics based on your organization's unique requirements. You'll discover how to quantify hard-to-measure security activities, compile and analyze all relevant data, identify strengths and weaknesses, set cost-effective priorities for improvement, and craft compelling messages for senior management.

Security Metrics successfully bridges management's quantitative viewpoint with the nuts-and-bolts approach typically taken by security professionals. It brings together expert solutions drawn from Jaquith's extensive consulting work in the software, aerospace, and financial services industries, including new metrics presented nowhere else. You'll learn how to:

• Replace nonstop crisis response with a systematic approach to security improvement
• Understand the differences between "good" and "bad" metrics
• Measure coverage and control, vulnerability management, password quality, patch latency, benchmark scoring, and business-adjusted risk
• Quantify the effectiveness of security acquisition, implementation, and other program activities
• Organize, aggregate, and analyze your data to bring out key insights
• Use visualization to understand and communicate security issues more clearly
• Capture valuable data from firewalls and antivirus logs, third-party auditor reports, and other resources
• Implement balanced scorecards that present compact, holistic views of organizational security effectiveness

Whether you're an engineer or consultant responsible for security and reporting

to management–or an executive who needs better information for decision-making–*Security Metrics* is the resource you have been searching for.

Andrew Jaquith, program manager for Yankee Group's Security Solutions and Services Decision Service, advises enterprise clients on prioritizing and managing security resources. He also helps security vendors develop product, service, and go-to-market strategies for reaching enterprise customers. He co-founded @stake, Inc., a security consulting pioneer acquired by Symantec Corporation in 2004. His application security and metrics research has been featured in *CIO*, *CSO*, *InformationWeek*, *IEEE Security and Privacy*, and *The Economist*.

Foreword
Preface
Acknowledgments
About the Author
Chapter 1 Introduction: Escaping the Hamster Wheel of Pain
Chapter 2 Defining Security Metrics
Chapter 3 Diagnosing Problems and Measuring Technical Security
Chapter 4 Measuring Program Effectiveness
Chapter 5 Analysis Techniques
Chapter 6 Visualization
Chapter 7 Automating Metrics Calculations
Chapter 8 Designing Security Scorecards
Index

Download Security Metrics: Replacing Fear, Uncertainty, and ...pdf

Read Online Security Metrics: Replacing Fear, Uncertainty, a ...pdf

Security Metrics: Replacing Fear, Uncertainty, and Doubt

By Andrew Jaquith

Security Metrics: Replacing Fear, Uncertainty, and Doubt By Andrew Jaquith

<>**The Definitive Guide to Quantifying, Classifying, and Measuring Enterprise IT Security Operations**

Security Metrics is the first comprehensive best-practice guide to defining, creating, and utilizing security metrics in the enterprise.

Using sample charts, graphics, case studies, and war stories, Yankee Group Security Expert Andrew Jaquith demonstrates exactly how to establish effective metrics based on your organization's unique requirements. You'll discover how to quantify hard-to-measure security activities, compile and analyze all relevant data, identify strengths and weaknesses, set cost-effective priorities for improvement, and craft compelling messages for senior management.

Security Metrics successfully bridges management's quantitative viewpoint with the nuts-and-bolts approach typically taken by security professionals. It brings together expert solutions drawn from Jaquith's extensive consulting work in the software, aerospace, and financial services industries, including new metrics presented nowhere else. You'll learn how to:

• Replace nonstop crisis response with a systematic approach to security improvement
• Understand the differences between "good" and "bad" metrics
• Measure coverage and control, vulnerability management, password quality, patch latency, benchmark scoring, and business-adjusted risk
• Quantify the effectiveness of security acquisition, implementation, and other program activities
• Organize, aggregate, and analyze your data to bring out key insights
• Use visualization to understand and communicate security issues more clearly
• Capture valuable data from firewalls and antivirus logs, third-party auditor reports, and other resources
• Implement balanced scorecards that present compact, holistic views of organizational security effectiveness

Whether you're an engineer or consultant responsible for security and reporting to management–or an executive who needs better information for decision-making–*Security Metrics* is the resource you have been searching for.

Andrew Jaquith, program manager for Yankee Group's Security Solutions and Services Decision Service, advises enterprise clients on prioritizing and managing security resources. He also helps security vendors develop product, service, and go-to-market strategies for reaching enterprise customers. He co-founded @stake, Inc., a security consulting pioneer acquired by Symantec Corporation in 2004. His application security and metrics research has been featured in *CIO*, *CSO*, *InformationWeek*, *IEEE Security and Privacy*, and *The Economist*.

Foreword
Preface
Acknowledgments

About the Author
Chapter 1 Introduction: Escaping the Hamster Wheel of Pain
Chapter 2 Defining Security Metrics
Chapter 3 Diagnosing Problems and Measuring Technical Security
Chapter 4 Measuring Program Effectiveness
Chapter 5 Analysis Techniques
Chapter 6 Visualization
Chapter 7 Automating Metrics Calculations
Chapter 8 Designing Security Scorecards
Index

Security Metrics: Replacing Fear, Uncertainty, and Doubt By Andrew Jaquith Bibliography

- Sales Rank: #526825 in Books
- Brand: Jaquith, Andrew
- Published on: 2007-04-05
- Released on: 2007-03-26
- Original language: English
- Number of items: 1
- Dimensions: 9.00" h x .90" w x 7.00" l, 1.19 pounds
- Binding: Paperback
- 336 pages

Download Security Metrics: Replacing Fear, Uncertainty, and ...pdf

Read Online Security Metrics: Replacing Fear, Uncertainty, a ...pdf

Preface

What This Book Is About

This book is about security metrics: how to quantify, classify, and measure information security operations in modern enterprise environments.

How This Book Came to Be

Every consultant worth his or her weight in receipts accumulates a small trove of metaphors, analogies, and witty expressions. These help explain or clarify those rarified things that consultants do and tend to lubricate the consulting process. Oh, and they also tend to be funny. One of my favorite bits—particularly relevant to the topic at hand—is this one:

> No good deed goes unpunished.

This simply means that with any worthwhile endeavor comes many unwitting (and often unwanted) consequences. So it is with the world of "security metrics." As you will see in the story I am about to tell you, my steadfast belief that security metrics ought to be a very! serious! field of study! has brought with it its own punishment.

Several years ago, several colleagues and I undertook a series of elaborate empirical studies on the subject of application security. We rigorously gathered and cleansed far-flung source material, aggregated and analyzed the resulting data, built an exotic mathematical model, and wrote a short research paper on the subject, complete with eye-catching charts and graphs. It was well received by customers and media alike. Some time later I was asked to present a condensed version of our findings on an Internet webcast run by an industry trade publication. In this case "webcast" meant a PowerPoint presentation accompanied by previously taped narration. The audience, as pitched to me by the sponsor, was to include "CSOs, technologists, and decision-makers."

That sounded great; I relished the opportunity to impress the bejeezus out of the vast numbers of grand globetrotters promised by the publication. In addition, my Inner Academic had high hopes that many in the audience would send me e-mails and letters marveling at the analytical techniques we used, the breadth of the data, and the many keen insights contained in the narrative and text. How wrong I was. Instead of measured praise from academe, I received several e-mails that went something like this:

> "Great presentation, but I was hoping to see more 'return on investment' numbers. You see, I really need to convince my boss to help me buy widget _____ (fill in the blank)."

And then there were the slightly more disturbing comments, like this one:

> "We have no money for our security program! Oh, woe is me! What I really need is more ROI! Help me!"

I confess to embroidering the truth a tiny bit here; the second e-mail I received was not nearly so plaintive.

But the theme was clear: viewers assumed that because the webcast was about "security metrics," it must be about ROI. Our marvelous metrics were the good deed; their unfulfilled expectations were the punishment.

Goals of This Book

Mercifully, the "security ROI" fad has gone the way of the Macarena. But to be absolutely sure that your expectations are managed (more consultantspeak for you), here is what this book is about, and what it is *not* about.

The primary objective of this book is to quantitatively analyze digital security activities. The chapters suggest ways of using numbers to illuminate an organization's security activities:

- **Measuring security:** Putting numbers around activities that have traditionally been considered difficult to measure
- **Analyzing data:** What kinds of sources of security data exist, and how you can put them to work for you
- **Telling a story:** Techniques you can use to marshal empirical evidence into a coherent set of messages

The need for a book like this seems plain to me. Security is one of the few areas of management that does not possess a well-understood canon of techniques for measurement. In logistics, for example, metrics such as "freight cost per mile" and "inventory warehouse turns" help operators understand how efficiently trucking fleets and warehouses run. In finance, "value at risk" techniques calculate the amount of money a firm could lose on a given day based on historical pricing volatilities. By contrast, security has . . . exactly nothing. No consensus on key indicators for security exists.

The lack of consensus on security metrics is, in part, due to the fact that the culture surrounding security is largely one of shame. Firms that get hacked tend not to talk about security incidents in public. Likewise, firms that are doing the right things tend not to talk either, lest giant red bull's-eyes appear on their firewalls' flanks. When they do talk, it is typically under NDA, or at small gatherings of like-minded people. Therefore, this book, as a secondary objective, documents effective practices of firms that take the responsibility of measuring their security activities seriously.

Non-goals of This Book

This book is first and foremost about *quantifying security activities*. It identifies ways to measure security processes that many enterprises consider important. The metrics and analysis techniques I document here are partly of my own devising but are drawn primarily from examples collected over the course of consulting in the software, aerospace, and financial services industries. I have met and exchanged notes with many people who have started their own metrics programs and are passionate about security metrics. At a minimum, I hope you will regard this book as a useful synthesis of current security measurement practices.

The word "practices" in that last sentence is important. I chose it carefully because of the implicit contrast with an opposing word: theory. In this book you will find plenty of anecdotes, lists of metrics, and ways of measuring security activities. But I have devoted only a small part of the text to *modeling* security risks—that is, figuring out which threats and risks are the right ones to worry about. Risk assessment is a broad field with many schools of thought. Smart people have spent many megawatts of brainpower modeling threats, modeling the effectiveness of security countermeasures, and simulating perimeter defenses.

The first non-goal of this book, therefore, is enterprise risk modeling and assessment. This is an important endeavor that every enterprise must undertake, but specific techniques are beyond the scope of this book. Risk assessment is an organization-specific activity, and I did not want to spend half of my pages

disclaiming things because "it depends on what risks your organization feels are the most important." Moreover, I did not wish to add to what is already an exceptionally rich canon of works devoted to the subject of risk modeling and assessment.

To this rather significant and somber-sounding non-goal I would like to add three more. The dearth of generally accepted security metrics often means that unscrupulous vendors manufacture blood-curdling statistics in a vacuum, devoid of context and designed to scare. Middle managers with agendas promptly recycle these metrics for their own purposes. Therefore, this book also is not about the following:

- **Budget justification:** How to convince your boss to spend money on security. If your company has not yet figured out that it needs to spend money on security, it likely has deeper problems than just a lack of statistics.
- **Fear, uncertainty, and doubt (FUD):** How to abuse or misrepresent data for the purpose of manufacturing security scare stories. I derive no pleasure from this, and it makes me feel cheap and dirty.
- **Funny money:** Any and all topics relating to "return on security investment." In addition to its dubious merit as a measure of security effectiveness, ROSI (as it is sometimes called) is a needless distraction from empirical security measurement.

Of course, because no good deed goes unpunished, it is entirely likely that this book will be used for those purposes regardless. But that, as a student of security analysis might say, is a risk worth taking.

Audience

I wrote this book for two distinct audiences: security practitioners and the bosses they report to. Practitioners need to know how, what, and when to measure. Their bosses need to know what to expect. Not for nothing has the security domain resisted measurement. As the bedraggled security manager of a household-name financial services firm recently told me, "My boss doesn't understand what I do every day. All he understands are numbers." Bridging the yawning gap between practitioners and management is what this book aims to achieve.

Overview of Contents

This book is divided into eight chapters:

- **Chapter 1, "Introduction: Escaping the Hamster Wheel of Pain":** The state of security metrics today eerily resembles a hamster wheel that spins continuously around an axis of vulnerability discovery and elimination. Thinking about security as a circular, zero-sum game cripples our ability to think clearly. This introductory chapter advocates replacing the hamster wheel with key indicators—metrics—that measure the efficiency of key security activities.
- **Chapter 2, "Defining Security Metrics":** This chapter describes the philosophy behind metrics, describes business pressures driving their adoption, suggests criteria for evaluating "good metrics," and warns against red herrings and other "bad metrics."
- **Chapter 3, "Diagnosing Problems and Measuring Technical Security":** Leading firms measure security activities differently, depending on need and context. This chapter catalogs the types of measurements that firms use to diagnose security problems. These include practical metrics for such topics as coverage and control, vulnerability management password quality, patch latency, benchmark scoring, and business-adjusted risk.
- **Chapter 4, "Measuring Program Effectiveness":** Beyond purely technical security measures, organizations need methods for measuring strategic security activities, for tracking security acquisition and implementation efforts, and for measuring the ongoing effectiveness of security organizations. This chapter

catalogs dozens of program-level metrics, using the COBIT framework as an organizing principle.

- **Chapter 5, "Analysis Techniques":** To create metrics, analysts must transform raw security data into numbers that provide richer insights. This chapter describes essential techniques for arranging, aggregating, and analyzing data to bring out the "headlines." It also describes advanced analytical techniques such as cross-sectional and quartile analyses.
- **Chapter 6, "Visualization":** Even the most compelling data is worthless without an effective way of presenting it. This chapter presents a myriad of visualization techniques, ranging from simple tables to two-by-two grids and intricate "small multiple" charts.
- **Chapter 7, "Automating Metrics Calculations":** Most organizations have plenty of security data available to them, although it is often trapped inside proprietary tools and information islands. This chapter suggests likely sources for finding appropriate data, including firewall logs, antivirus logs, and third-party auditor reports. It also describes techniques for transforming acquired data into formats that lend themselves to aggregation and reporting.
- **Chapter 8, "Designing Security Scorecards":** After an organization collects and analyzes its security metrics, only one step remains: creating a scorecard that pulls everything together. This chapter presents several alternative approaches for designing security "balanced scorecards" that present compact, holistic views of organizational security effectiveness.

In addition to these topics, this book contains a generous sprinkling of anecdotes and war stories from my personal experiences, as well as those of my interview subjects.

Thank you for purchasing this book. I hope you enjoy reading it as much as I have enjoyed writing it.

© Copyright Pearson Education. All rights reserved.

Read Security Metrics: Replacing Fear, Uncertainty, and Doubt By Andrew Jaquith for online ebook

Security Metrics: Replacing Fear, Uncertainty, and Doubt By Andrew Jaquith Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read Security Metrics: Replacing Fear, Uncertainty, and Doubt By Andrew Jaquith books to read online.

Online Security Metrics: Replacing Fear, Uncertainty, and Doubt By Andrew Jaquith ebook PDF download

Security Metrics: Replacing Fear, Uncertainty, and Doubt By Andrew Jaquith Doc

Security Metrics: Replacing Fear, Uncertainty, and Doubt By Andrew Jaquith Mobipocket

Security Metrics: Replacing Fear, Uncertainty, and Doubt By Andrew Jaquith EPub