DOUGLAS W. HUBBARD
& RICHARD SEIERSEN

HOW TO MEASURE ANYTHING IN CYBERSECURITY RISK

Forewords by
DANIEL E. GEER, JR.
& STUART MCCLURE

WILEY

How to Measure Anything in Cybersecurity Risk

DOUGLAS W. HUBBARD
RICHARD SEIERSEN

WILEY

Cover images: Cyber security lock © Henrik5000/iStockphoto; Cyber eye © kasahasa/iStockphoto; Internet Security concept © bluebay2014/iStockphoto; Background © omergenc/iStockphoto; Abstract business background © Natal'ya Bondarenko/iStockphoto; Abstract business background © procurator/iStockphoto; Cloud Computing © derrrek/iStockphoto
Cover design: Wiley

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data:
ISBN 978-1-119-08529-4 (Hardcover)
ISBN 978-1-119-22460-0 (ePDF)
ISBN 978-1-119-22461-7 (ePub)

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

Douglas Hubbard's dedication: To my children, Evan, Madeleine, and Steven, as the continuing sources of inspiration in my life; and to my wife, Janet, for doing all the things that make it possible for me to have time to write a book, and for being the ultimate proofreader.

Richard Seiersen's dedication: To all the ladies in my life: Helena, Kaela, Anika, and Brenna. Thank you for your love and support through the book and life. You make it fun.

Doug and Richard would also like to dedicate this book to the military and law enforcement professionals who specialize in cybersecurity.

Foreword

Daniel E. Geer, Jr., ScD

Daniel Geer is a security researcher with a quantitative bent. His group at MIT produced Kerberos, and a number of startups later he is still at it—today as chief information security officer at In-Q-Tel. He writes a lot at every length, and sometimes it gets read. He's an electrical engineer, a statistician, and someone who thinks truth is best achieved by adversarial procedures.

It is my pleasure to recommend *How to Measure Anything in Cybersecurity Risk*. The topic is nothing if not pressing, and it is one that I have myself been dancing around for some time.[1] It is a hard problem, which allows me to quote Secretary of State John Foster Dulles: "The measure of success is not whether you have a tough problem to deal with, but whether it is the same problem you had last year." At its simplest, this book promises to help you put some old, hard problems behind you.

The practice of cybersecurity is part engineering and part inference. The central truth of engineering is that design pays if and only if the problem statement is itself well understood. The central truth of statistical inference is that all data has bias—the question being whether you can correct for it. Both engineering and inference depend on measurement. When measurement gets good enough, metrics become possible.

I say "metrics" because metrics are derivatives of measurement. A metric encapsulates measurements for the purpose of ongoing decision support. I and you, dear reader, are not in cybersecurity for reasons of science, though those who are in it for science (or philosophy) will also want measurement of some sort to backstop their theorizing. We need metrics derived from solid measurement because the scale of our task compared to the scale of our tools demands force multiplication. In any case, no game play improves without a way to keep score.

Early in the present author's career, a meeting was held inside a market-maker bank. The CISO, who was an unwilling promotion from Internal

[1] We are fortunate to have two forewords from two leading thinkers in cybersecurity risk assessment—Daniel E. Geer, Jr., and Stuart McClure.

Audit, was caustic even by the standards of NYC finance. He began his comments mildly enough:

> Are you security people so stupid that you can't tell me:
> - How secure am I?
> - Am I better off than I was this time last year?
> - Am I spending the right amount of money?
> - How do I compare to my peers?
> - What risk transfer options do I have?

Twenty-five years later, those questions remain germane. Answering them, and others, comes only from measurement; that is the "Why?" of this book.

Yet even if we all agree on "Why?," the real value of this book is not "Why?" but "How?": *how* to measure and then choose among methods, *how* to do that both consistently and repeatedly, and *how* to move up from one method to a better one as your skill improves.

Some will say that cybersecurity is impossible if you face a sufficiently skilled opponent. That's true. It is also irrelevant. Our opponents by and large pick the targets that maximize their return on their investment, which is a polite way of saying that you may not be able to thwart the most singularly determined opponent for whom cost is no object, but you can sure as the world make other targets more attractive than you are. As I said, no game play improves without a way to keep score. That is what this book offers you—a way to improve your game.

This all requires numbers because numbers are the only input to both engineering and inference. Adjectives are not. Color codes are not. If you have any interest in taking care of yourself, of standing on your own two feet, of knowing where you are, then you owe it to yourself to exhaust this book. Its writing is clear, its pedagogy is straightforward, and its downloadable Excel spreadsheets leave no excuse for not trying.

Have I made the case? I hope so.

Note

1. Daniel Geer, Jr., Kevin Soo Hoo, and Andrew Jaquith, "Information Security: Why the Future Belongs to the Quants," *IEEE Security & Privacy* 1, no. 4 (July/August 2003): 32–40, geer.tinho.net/ieee/ieee.sp.geer.0307.pdf.

Foreword

Stuart McClure

Stuart McClure is the CEO of Cylance, former global CTO of McAfee, and founding author of the *Hacking Exposed* series.

My university professors always sputtered the age-old maxim in class: "You can't manage what you cannot measure." And while my perky, barely-out-of-teenage-years ears absorbed the claim aurally, my brain never really could process what it meant. Sure, my numerous computer science classes kept me chasing an infinite pursuit of improving mathematical algorithms in software programs, but little did I know how to really apply these quantitative efforts to the management of anything, much less cyber.

So I bounded forward in my career in IT and software programming, looking for an application of my unique talents. I never found cyber measurement all that compelling until I found cybersecurity. What motivated me to look at a foundational way to measure what I did in cybersecurity was the timeless question that I and many of you get almost daily: "Are we secure from attack?"

The easy answer to such a trite yet completely understandable question is "No. Security is never 100%." But some of you have answered the same way I have done from time to time, being exhausted by the inane query, with "Yes. Yes we are." Why? Because we know a ridiculous question should be given an equally ridiculous answer. For how can we know? Well, you can't—without metrics.

As my cybersecurity career developed with InfoWorld and Ernst & Young, while founding the company Foundstone, taking senior executive roles in its acquiring company, McAfee, and now starting Cylance, I have developed a unique appreciation for the original professorial claim that you really cannot manage what you cannot measure. While an objective metric may be mythical, a subjective and localized measurement of your current risk posture and where you stand relative to your past and your peers is very possible.

Measuring the cyber risk present at an organization is nontrivial, and when you set the requirement of delivering on quantitative measurements rather than subjective and qualitative measurements, it becomes almost beyond daunting.

The real questions for all of us security practitioners are ultimately "Where do we start? How do we go about measuring cybersecurity's effectiveness and return?" The only way to begin to answer those questions is through quantitative metrics. And until now, the art of cybersecurity measurement has been elusive. I remember the first time someone asked me my opinion on a security-risk metrics program, I answered something to the effect of, "It's impossible to measure something you cannot quantify."

What the authors of this book have done is begin to define a framework and a set of algorithms and metrics to do exactly what the industry has long thought impossible, or at least futile: measure security risk. We may not be perfect in our measurement, but we can define a set of standard metrics that are defensible and quantifiable, and then use those same metrics day in and day out to ensure that things are improving. And that is the ultimate value of defining and executing on a set of security metrics. You don't need to be perfect; all you need to do is start somewhere and measure yourself relative to the day before.

Acknowledgments

We thank these people for their help as we wrote this book:

- Jack Jones
- Jack Freund
- Jim Lipkis
- Thomas Lee
- Christopher "Kip" Bohn
- Scott Stransky
- Tomas Girnius
- Jay Jacobs
- Sam Savage
- Tony Cox
- Michael Murray
- Patrick Heim
- Cheng-Ping Li
- Michael Sardaryzadeh
- Stuart McClure
- Rick Rankin
- Anton Mobley
- Vinnie Liu
- SIRA.org Team
- Dan Geer
- Dan Rosenberg

A very special thanks to Bonnie Norman and Steve Abrahamson for providing additional editing.

About the Authors

Douglas Hubbard is the creator of the Applied Information Economics method and the founder of Hubbard Decision Research. He is the author of one of the best-selling business statistics books of all time, *How to Measure Anything: Finding the Value of "Intangibles" in Business*. He is also the author of *The Failure of Risk Management: Why It's Broken and How to Fix It*, and *Pulse: The New Science of Harnessing Internet Buzz to Track Threats and Opportunities*. He has sold more than 100,000 copies of his books in eight different languages, and his books are used in courses at many major universities. His consulting experience in quantitative decision analysis and measurement problems totals over 27 years and spans many industries including pharmaceuticals, insurance, banking, utilities, cybersecurity, interventions in developing economies, mining, federal and state government, entertainment media, military logistics, and manufacturing. He is also published in several periodicals including *Nature*, *The IBM Journal of R&D*, *Analytics*, *OR/MS Today*, *InformationWeek*, and *CIO Magazine*.

Richard Seiersen is a technology executive with nearly 20 years of experience in information security, risk management, and product development. Currently he is the general manager of cybersecurity and privacy for GE Healthcare. Many years ago, prior to his life in technology, he was a classically trained musician—guitar, specifically. Richard now lives with his family of string players in the San Francisco Bay Area. In his limited spare time he is slowly working through his MS in predictive analytics at Northwestern. He should be done just in time to retire. He thinks that will be the perfect time to take up classical guitar again.

Contents

Introduction

Why This Book, Why Now?

This book is the first of a series of spinoffs from Douglas Hubbard's successful first book, *How to Measure Anything: Finding the Value of "Intangibles" in Business*. For future books in this franchise, we were considering titles such as *How to Measure Anything in Project Management* or industry-specific books like *How to Measure Anything in Healthcare*. All we had to do was pick a good idea from a long list of possibilities.

Cybersecurity risk seemed like an ideal first book for this new series. It is extremely topical and filled with measurement challenges that may often seem impossible. We also believe it is an extremely important topic for personal reasons (as we are credit card users and have medical records, client data, intellectual property, and so on) as well as for the economy as a whole.

Another factor in choosing a topic was finding the right co-author. Because Doug Hubbard—a generalist in measurement methods—would not be a specialist in any of the particular potential spinoff topics, he planned to find a co-author who could write authoritatively on the topic. Hubbard was fortunate to find an enthusiastic volunteer in Richard Seiersen—someone with years of experience in the highest levels of cybersecurity management with some of the largest organizations.

So, with a topical but difficult measurement subject, a broad and growing audience, and a good co-author, cybersecurity seemed like an ideal fit.

What Is This Book About?

Even though this book focuses on cybersecurity risk, this book still has a lot in common with the original *How to Measure Anything* book, including:

1. Making better decisions when you are significantly uncertain about the present and future, and
2. Reducing that uncertainty even when data seems unavailable or the targets of measurement seem ambiguous and intangible.

This book in particular offers an alternative to a set of deeply rooted risk assessment methods now widely used in cybersecurity but that have no basis in the mathematics of risk or scientific method. We argue that these methods impede decisions about a subject of growing criticality. We also argue that methods based on real evidence of improving decisions are not only practical but already have been applied to a wide variety of equally difficult problems, including cybersecurity itself. We will show that we can start at a simple level and then evolve to whatever level is required while avoiding problems inherent to "risk matrices" and "risk scores." So there is no reason not to adopt better methods immediately.

What to Expect

You should expect a gentle introduction to measurably better decision making—specifically, improvement in high-stakes decisions that have a lot of uncertainty and where, if you are wrong, your decisions could lead to catastrophe. We think security embodies all of these concerns.

We don't expect our readers to be risk management experts or cybersecurity experts. The methods we apply to security can be applied to many other areas. Of course, we do hope it will make those who work in the field of cybersecurity better defenders and strategists. We also hope it will make the larger set of leaders more conscious of security risks in the process of becoming better decision makers.

Is This Book for Me?

If you really want to be sure this book is for you, here are the specific personas we are targeting:

- You are a decision maker looking to improve—that is, *measurably improve*—your high-stakes decision making.
- You are a security professional looking to become more strategic in your fight against the bad guy.
- You are neither of the above. Instead, you have an interest in understanding more about cybersecurity and/or risk management using readily accessible quantitative techniques.

- If you are a hard-core quant, consider skipping the purely quant parts. If you are a hard-core hacker, consider skipping the purely security parts. That said, we will often have a novel perspective, or "epiphanies of the obvious," on topics you already know well. Read as you see fit.

We Need More Than Technology

We need to lose less often in the fight against the bad guys. Or, at least, lose more gracefully and recover quickly. Many feel that this requires better technology. We clamor for more innovation from our vendors in the security space even though breach frequency has not been reduced. To effectively battle security threats, we think there is something equally important as innovative technology, if not more important. We believe that "something" must include a better way to think quantitatively about risk.

New Tools for Decision Makers

We need decision makers who consistently make better choices through better analysis. We also need decision makers who know how to deftly handle uncertainty in the face of looming catastrophe. Parts of this solution are sometimes referred to with current trendy terms like "predictive analytics," but more broadly this includes all of decision science or decision analysis and even properly applied statistics.

Our Path Forward

Part I of this book sets the stage for reasoning about uncertainty in security. We will come to terms on things like security, uncertainty, measurement, and risk management. We also argue against toxic misunderstandings of these terms and why we need a better approach to measuring cybersecurity risk and, for that matter, measuring the performance of cybersecurity risk analysis itself. We will also introduce a very simple quantitative method that could serve as a starting point for anyone, no matter how averse they may be to complexity.

Part II of this book will delve further into evolutionary steps we can take with a very simple quantitative model. We will describe how to add further complexity to a model and how to use even minimal amounts of data to improve those models.

Last, in Part III we will describe what is needed to implement these methods in the organization. We will also talk about the implications of this book for the entire cybersecurity "ecosystem," including standards organizations and vendors.

PART I

Why Cybersecurity Needs Better Measurements for Risk