Security Metrics: Replacing Fear, Uncertainty, and Doubt
Andrew Jaquith
Addison Wesley, 2007
$49.99 (paper), 306 pp.
ISBN 0-32-134998-9

Review by Joel Rosenblatt

Building a successful IT security program is a complicated and sometimes frustrating task. Showing the program's effectiveness is tricky because, by definition, if your program works well, you have nothing to measure. When you have something to measure, it usually results from a failure in security, which is not something you want to show off to your boss. The idea of measuring success by showing that less and less happened is fascinating to me, and it prompted my interest in security metrics.

I have always been interested in the Heisenberg Uncertainty Principle, loosely defined as the inability to measure something without changing it. I always thought you should be able to improve security as a result of measuring it. The converse of this would also be true—if you can't measure security, you can never improve it.

Once I convinced myself that in order to build a successful security program, I would have to start collecting and using security metrics, I began to look for people and organizations that were talking about this problem. This led me to securitymetrics.org. Andrew Jaquith is the moderator and driving force behind the securitymetrics.org mailing list, and his experience in the computer security business extends over 20 years. Readers of his well-written but easygoing prose see clearly that he knows his subject. While the book is about security metrics, it also includes a lot of information about computer security—or, should I say, how computer security could (and in some cases should) be done.

Jaquith begins his book with "Escaping the Hamster Wheel of Pain," an entertaining analysis of the structure of many a security program. He talks about a "cynical version" of risk management, in which you discover a problem, panic, explain to the boss why the problem arose, patch up the problem, and hope it doesn't come back.

He then dives into "Defining Security Metrics," an area essential for anyone looking to understand and build a security metrics program. Everyone has a different understanding of security and what needs to be done for an organization's management to feel secure. This chapter will help you build a picture of what metrics are, what kinds of things need to be measured, and how to make sure that the data you collect will be useful.

The next two chapters, "Diagnosing Problems and Measuring Technical Security" and "Measuring Program Effectiveness," got me thinking that the subtitle of the book should be modified to "Replacing Fear, Uncertainty, and Doubt with Terror." Jaquith starts to look at various security programs and how to figure out if they are working. By the end of these chapters, you appreciate his mastery of the topic and understand why it is so hard to get it right. Jaquith points out that there is a big difference between "fun facts"—like how many probes your firewall blocked, which is an interesting number but not really a security metric—and data such as how many systems on your network launched attacks, which is a much better measure of the effectiveness of your security program. With IT security, you can work very hard or very smart—and sometimes both. It is possible to appear to be working hard (and, in fact, doing a lot of work) but adding very little to the security of the organization. These chapters will help you make the right decisions about where you should put your time and effort.

Chapters five and six, "Analysis" and "Visualization," are a mini course on statistics and how to properly display data. If you have never taken a class on statistical methods or display graphics, these chapters will provide a good basis for understanding them. If you are a statistical genius, you can probably skip chapter five, and you may find yourself arguing with chapter six. Jaquith tends to be a graphical purest: he believes in very clear and clean graphical representations of data and strongly resists, for example, three-dimensional charts, saying that "the artificial depth only distracts the viewer from the data." Nevertheless, there is some really good information in there. The section on "label honestly and without contortions" makes some excellent points on how bad or missing labels can completely obscure the meaning of the data.

By this point, you will feel ready to get out there and start measuring things. Chapter seven, "Automating Metrics Calculations," will give you the tools needed to build a metrics program that will produce consistent and repeatable results. One of the things that becomes obvious to anyone involved in computer security is that the amount of information produced by any security system is enormous. In order to end up with any usable intelligence, automation is essential.

The last chapter, "Designing Security Scorecards," shows you how to make all of the hard work you've done produce results that will be understandable to the non-security executives at your organization.

Computer security people are usually either heroes or in the doghouse. Having a viable security metrics program that produces results that are understandable throughout the organization is a goal worthy of your time and effort. This book will kick-start your effort and help you stay out of the doghouse. e

Joel Rosenblatt (joel@columbia.edu) is Manager of Computer and Network security for Columbia University. He currently chairs the Security Metrics subcommittee of the EDUCAUSE Effective Practices committee.

Educator's Podcast Guide
Bard Williams
International Society for Technology in Education, 2007
$22.35 (ISTE member), $31.95 (nonmember); 290 pp.
978-1-56484-231-2

Reviewed by R. Martin Reardon

The opening section of the ISTE publication *Educator's Podcast Guide* by Bard Williams declares that the book is "for anyone who's involved in using, supporting, or evangelizing technology in an educational institution." To continue with the evangelizing analogy, Williams is clearly one of the faithful. His enthusiasm for this topic is contagious, and he maintains his upbeat approach as he rhetorically inquires of his readers in Part One, "What are you waiting for?" The three chapters in Part One constitute the theoretical foundation of the book, and I will return to discussing them shortly.

Part Two (chapters 4 through 15) consists of Williams's selection of and commentary on a number of exemplary podcast sites relevant to a wide range of teaching situations, from higher education to K–12 science, mathematics, English/language arts, social sciences and fine arts, foreign languages, and news reports. With a separate chapter dedicated to each of the "content" areas, Williams utilizes a template format occupying two facing pages so that the reader can quickly scan for useful information and find it in the same location for each podcast site. The easy-to-follow two-page template spread commences with the URL and a screen shot of the podcast site, followed by a concise and perceptive description of the podcast's focus, suggestions for classroom applications, and general information such as the suggested audience, whether the podcast is video or audio or both, and the source and frequency of the podcast.

The twelve chapters of Part Two enshrine Williams's "obsession"—choosing from among thousands of podcasts the ones he believes are "the right ones for this book." And what wonderful sites he has ferreted out! I found many that have now become added to my iTunes library. Even for someone who is already adept at creating podcasts, the sites discussed in Part Two make this book worth its purchase price. These chapters are better regarded as a great place for the reader to start looking for the perfect resource to fill a particular need, rather than as a series of chapters to be read sequentially.

In Part One, Williams sets about demystifying podcasting. He understands that "to many people, podcasting seems like magic," but his project is to provide concise information that will ensure that his reader approaches podcasting "knowing the right things about the task in hand." Williams is keenly aware of how quickly newcomers to podcasting can be overwhelmed by jargon and mysterious acronyms like RSS, and he strikes a fine balance by providing enough detail to make the concepts clear while refraining from unleashing the full force of his technical expertise. For example, in defining the term "podcast," he provides a plain English definition and avoids complexity and the reinvention of the wheel by simply referring the inquisitive reader to the Wikipedia entry on podcasting.

Even in the supportive and comfortable context of the faculty learning community (FLC) where I learned how to create podcasts, Williams's book would have been a welcome guide, both for those of us learning the technology and for the FLC leader. Williams offers many practical hints for those who decide to produce podcasts. These range from choosing a reasonably quiet recording room (perhaps a storeroom) to spreading the word about the produced podcast (perhaps by means of a blog). He suggests a standard format for producing a podcast that, until reading his description, I had not realized was used by a number of my favorite podcast sources. He highlights the importance of assessing the educational value of any podcast used in the classroom. He provides two rubrics for evaluating podcasts, suggesting their use as discussion starters around the pivotal issue of how to determine quality in podcasting. Williams is very aware of the existence of marginal podcasts, and his provision of clear guidelines, which he refrains from trying to set in stone, is most helpful.

These days, it is hard for me to accurately recall my fears about podcasting: that I would be inordinately frustrated by my ignorance, and that I would ultimately see very little return for the considerable investment of time required. I recommend Williams's book for anyone who identifies with my former fears and who is considering either using or producing podcasts in an educational environment. *Educator's Podcast Guide* is so helpful that I will forgive Williams for omitting one of my favorite podcasts from his listing: TED Talks (http://www.ted.com/talks). e

R. Martin Reardon (rmreardon@vcu.edu) is Assistant Professor, Educational Leadership Department, in the School of Education at Virginia Commonwealth University in Richmond.

Recommend Books

The Recommended Reading department of *EDUCAUSE Quarterly* highlights recent books that offer practical advice or insight for campus practitioners including network administrators, instructional technologists, IT leaders, faculty, librarians, and others. Reviewed books cover a wide range of topics, such as security, infrastructure, help desks, leadership, and teaching and learning.

A review should
- be about 1,000 words,
- demonstrate how and how well the book covers an IT issue, and
- explain how the information is broadly applicable.

To recommend a book or volunteer to write a review, contact editor Gregory Dobbin at gdobbin@educause.edu with a proposal.