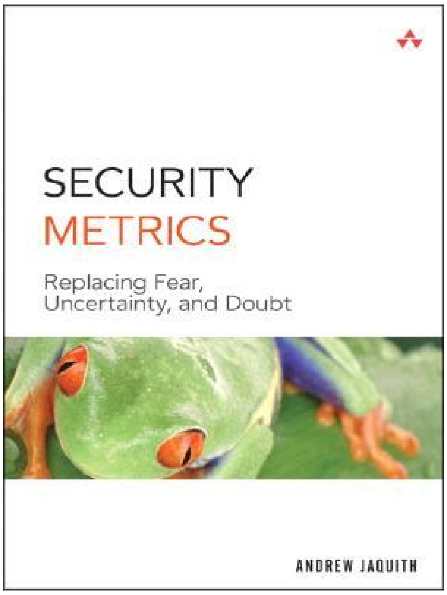

Security Metrics: Replacing Fear, Uncertainty, and Doubt

Andrew Jaquith

Security Metrics: Replacing Fear, Uncertainty, and Doubt

Andrew Jaquith

Security Metrics: Replacing Fear, Uncertainty, and Doubt 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*.

Security Metrics: Replacing Fear, Uncertainty, and Doubt Details

Date	:	Published March 1st 2007 by Addison-Wesley Professional
ISBN	:	9780321349989
Author	:	Andrew Jaquith
Format	:	Paperback 306 pages
Genre	:	Science, Technology, Computer Science, Nonfiction

Download and Read Free Online Security Metrics: Replacing Fear, Uncertainty, and Doubt Andrew Jaquith

From Reader Review Security Metrics: Replacing Fear, Uncertainty, and Doubt for online ebook

Nick says

As I said on Amazon.com, I liked it better than Cats! Security Metrics. It's interesting to read this and then talk to bankers and other end users of IT and see how it maps against the realities of the IT budgeting process. But Andy can write, and he knows his stuff, cold.

Dan says

A for effort. It's hard to quantify some of this stuff, and for everyone who likes to poke holes in the logic, no one has proposed a better solution....

John Johnson says

A few years old now, but still very relevant. Highly recommended. I will be using this in my Walden Information Assurance and Risk Management class to emphasize the importance of using meaningful metrics well, and communicating them properly.

Rick Howard says

From my Terebrate Blog Site: http://terebrate.blogspot.com

Executive Summary

This book is a must-read for all cyber security professionals. It is not a part of the canon because it attacks a sacred cow of the industry—Annualized Loss Expectancy (ALE) as a means to justify your security budget—and the community has yet to fully embrace the idea that ALE might not be a good idea in all cases. But you should seriously consider this notion and this book is your gateway to do so. Consider it a Canon-Candidate. Jaquith describes why capturing and analyzing security metrics is a good and powerful thing and how you can use that intelligence to better understand the porous nature of your networks. It will help you unshackle yourself from the chains of probabilistic risk assessments. It will turn you away from the dark side and toward a more meaningful process to assess your enterprise’s security. You should have read this by now.

Introduction

I have been interested in cyber security metrics and how to visualize them since before we were connecting the Internet with strings and soup cans. In 2011, I had been looking for somebody to put some rigor to the idea when I stumbled upon a strong, positive review of Jaquith’s book by Richard Bejtlich on Amazon.[1] For those unfamiliar with Bejtlich, his security blog—TaoSecurity—is one of the best out there.[2] You would do well to put it in your regular reading rotation. He has been a prolific reader and reviewer of security books, and although his production has dropped off since he became the Mandiant CSO, I am still a fan and read everything that he writes. His recommendations, both positive and negative, tend to skew toward the practical. He does not have a lot of use for pie-in-the-sky nonsense. Unless you can apply it in the real world, Bejtlich has no use for it. When I read his positive review of Jaquith's book, I became excited.

The Tech

From the beginning, Jaquith attacks the security community's sacred cow of applying ALE to convince management that the security program it is paying for is working. I have to say that I loved this attack. I remember first learning about ALE when I was studying for the Certified Information Systems Security Professional (CISSP) exam back in the day. I thought then that ALE sounded well and good when you said it fast, but in reality, you were just making up the numbers to plug into a formula that sounded scientific.

According to Jaquith, and every CISSP preparatory exam book on the planet,

"ALE is the monetary loss that can be expected for an asset due to a risk over a 1-year period and is calculated by multiplying the single loss expectancy (SLE) by the annualized rate of occurrence (ARO)." [6]

Doesn't that sound precise and mathematical? Indeed it does, and therefore it must be correct. It turns out though that there are lots of problems with this formula. The biggest problem is that we don't know what the probabilities are. How can we possibly know what the probability is that an advanced-persistent-threat-style attack will compromise the computer that your chief of counsel's secretary uses? This is not the insurance industry; we do not have actuary tables derived from decades of data collection that can tell us precisely what these adversaries will do, how often they will do it and how much it will cost us when they do it. What do ALE practitioners do in the absence of hard data? They guess. They estimate. They fudge. And when they do this, they undermine the veracity of the very process that they are trying to convince management is so exacting. What good is a scientific formula if all you do is fill it with garbage data?

Jaquith's thesis is that, instead of using imprecise models like ALE, security professionals should use metrics instead. He says that,

"[this change in thinking] requires practitioners to think about security in the same way that other disciplines do – as activities that can be named, and whose efficiencies can be measured with key indicators." [6]

Coincidentally, the first time I read Jaquith's book, I just happened to listen to the Patrick Gray Risky Business podcast where he interviewed Brian Snow.[3] Brian Snow is a former NSA information assurance technical director, and he had a lot to say about the folly of using probabilistic risk assessments, like ALE, to improve the cost-effectiveness of securing nuclear facilitates and government information assurance programs. Snow made the point that these models are fine for standard risks that routinely occur—like what is the mean time to failure of the hard drive in your laptop—but that they fail miserably when trying to predict cases that have high impact to an organization but are not likely to occur. These cases that Snow referred to are called "black swan events."

Black swan events were made famous by Nassim Nicholas Taleb in his book The Black Swan: The Impact of the Highly Improbable, published in 2007. For some organizations, computer breaches are black swan events that Taleb describes as "outliers that carry extreme impact."[5] They are outliers because the chances of something like that happening to your network are pretty small, but when it does, the cost to your organization is extreme.

Jaquith’s solution is to

“… quantify, classify, and measure information security operations in a modern enterprise environment” and to provide “… a set of key indicators that tell customers how healthy their security operations are.” [6]

He spends a good portion of his book, two entire chapters actually, explaining what some of these metrics might be. Your organization might not have a use for all of them, but you will appreciate the thoroughness that Jaquith uses to explain why they should be considered. Chapters three and four are well worth the read.

As a bonus, he spends a chapter reviewing the fundamentals of statistics. If you are like me and slept through your probability and statistics course in college, you will welcome this refresher. His simple explanation alone about what a standard deviation is and what correlation really means is worth the price of admission.

As an extra bonus, he spends a chapter on visualization. I am a fan of Dr. Edward Tufte,[4] who is in my opinion the world’s leading expert on how to visually display complex data. Tufte devotees will learn nothing new here but will appreciate how Jaquith reduces Tufte’s four seminal books on the subject to six rules:

It’s about the data, not the design.
Just say no to three-dimensional graphics and cutesy chart junk.
Don’t go off to meet the (Microsoft) wizard.
Erase, erase, erase.
Reconsider Technicolor.
Label honestly and without contortions." [6]

The only fault I have with the book is the last chapter, “Designing Security Scorecards.” Here, Jaquith had the opportunity to show some practical security dashboards that perhaps some real organization used and found useful. Instead, he spends the entire chapter explaining what goes into making a scorecard. As I got closer to the end of the book, I just knew that I was going to see some dazzling examples that I might use in my own organization. When I turned to the last page and found nothing but the index, I was dumbfounded. He provided no examples of real-world security dashboards. D’oh! So close to being perfect!

Conclusion

That one caveat aside, Jaquith’s book is well worth the read. I recommend it highly. I dare you to get to the end of that book without learning something that will help you in your current job. If security metrics are not your thing, then statistics and visualization will make you a more well-rounded business person. But for you security professionals out there, this book is for you. It will help you unshackle yourself from the chains of probabilistic risk assessments. It will turn you away from the dark side and toward a more meaningful process to assess your enterprise’s security. You should have read this by now.

Note

I worked for iDefense (a VeriSign Inc. business unit) the first time that I wrote a book review of Security Metrics. Jason Greenwood, the current general manager and an old friend of mine, has graciously allowed me to reuse some of the original content from that review for this updated blog post. iDefense is still one of the best commercial cyber security intelligence outfits out there. If you have cyber intelligence needs, you should consider calling those guys.

Sources

[1] “A ground-breaking book that all security managers should read,” August 9, 2007, by Richard Bejtlich “TaoSecurity,” Amazon, Last Visited 28 November 2013,
http://www.amazon.com/review/R2MKJYGL...

[2] “TaoSecurity,” by Richard Bejtlich, Last Visited 28 November 2013,
http://taosecurity.blogspot.com/

[3] "Risky Business #191 -- Nuclear weapons security and infosec," by Patrick Gray, 15 April 2011, Last Visited 28 November,
http://risky.biz/RB191

[4] "The Work of Edward Tufte and Graphic Press," by Edward Tufte, Last Visited 28 November 2013,
http://www.edwardtufte.com/tufte/index

[5] "The Black Swan: The Impact of the Highly Improbable," by Nassim Nicholas Taleb, Random House, 17 April 2007.

[6] "Security Metrics: Replacing Fear, Uncertainty, and Doubt,"
by Andrew Jaquith, Published by Addison-Wesley ProfessionalMarch 2007

References

"Fresh, compelling take on information security metrics," by Richard Bejtlich "TaoSecurity,” Amazon, 22 August 2010, Last Visited 2 December 2013,

---

Ivars Svekris says

Insightful.
