PRAGMATIC Security Metrics:
Applying Metametrics to Information Security

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
School of Business & Management
Norwich University

Recently I was surprised to be asked to write the Preface to a new book: W. Krag Brotby and Gary Hinson's *Pragmatic Security Metrics: Applying Metametrics to Information Security* (CRC Press – Taylor & Francis Group, 2013 (ISBN 978-1-4398-8152-1; xviii + 494; index)< http://www.amazon.com/PRAGMATIC-Security-Metrics-Metametrics-Information/dp/1439881529 >. After reading the galley proofs, here's what I wrote (using US spelling):

> Information assurance (IA) has suffered for decades from the lack of sound quantitative methods for coping with risk and evaluating alternative strategies for allocating resources wisely in the fight against errors and attacks on our information systems.
>
> All of us involved in IA maneuver through competing frameworks for choosing and implementing defenses; unfortunately, all too often we rely on the equivalent of word-of-mouth recommendations – industry best practices – in choosing particular paths. As our field matures, we must learn from other professions where methods for evaluating the quality of approaches have shifted from purely intuitive approaches to more systematic and repeatable methods.
>
> The authors of this book have contributed their experience and creativity to present a valuable methodology for creating and evaluating elements of security management. Throughout the work, they emphasize how important it is to use heuristics rather than rigid rules in any field that changes constantly.
>
> Security of all kinds suffers from the fundamental difficulty that if security measures work, there's less evidence that the measures were necessary, at least for non-professional observers such as non-technical managers. Without sound metrics, we are in the position of passersby who encounter a man swinging plucked chickens around his head while he stands on a street corner: asked why he is doing that, he answers, "To keep the flying elephants away." "But there are no flying elephants," respond the befuddled observers. He crows triumphantly, "See? It works!"
>
> Without defining, testing and refining metrics, our profession will continue to be subject to the legitimate question, "How do you know?" How do we know if our proposals – our proposed spending, our proposed topology, our proposed changes – are reasonable? Why do we choose one set of responses over another? And how will we measure the results of our methods to evaluate their effectiveness and their efficiency?
>
> In addition to supporting the development of IA, the methods presented in this text will reach professionals in fields that will benefit from good, PRAGMATIC metrics.
>
> Thanks to Krag Brotby and Gary Hinson, I expect to see dramatic changes in our ability

to analyze our security options, explain our choices, and measure our results.

I received my free copy of the book a few weeks ago and want to let readers know about it. I really like the "Office Memorandum" on pp xvii & xviii, which looks like one of my own examination questions: it's a request from a chief executive officer to the information security manager and it asks for a written explanation of

- What's the return on investment of the spending on information security over the last three years?
- How does the company's information security program compare with those of comparable companies in their industry?
- Are they spending too much on information security?
- If they have to cut expenditures, what aspects of the information security efforts could reasonably be reduced?

These questions echo those I have insisted for years must be answered at any time by a security manager:

- What are we doing and how much are we spending on information security?
- Why have you decided that we don't need to do and spend more?
- Why have you decided that we don't need to do and spend less?

Answering these questions without methods for measuring our efforts – that is, having *metrics* – is difficult. Without metrics, we're reduced to guesswork and intuition. The authors specifically use the following pragmatic definitions which are interesting in themselves:

- Governance: the act of governing through mandating a set of rules and regulations regarding the actions of individuals within the organization, plus the directive, control, and feedback processes to ensure their compliance.
- Indicator: something that gives an indication, that is, an indirect, vague, and/ or imprecise measure that may not be strongly correlated with the subject of measurement.
- Instrument: short for "measuring instrument," that is, a device for measuring.
- Measure: (verb) to determine one or more parameters of something; (noun) short for measurement, for example, the meter ("metre" outside the United States) is a length measure.
- Measurement: the value of a parameter for something, ideally expressed in defined units with an appropriate degree of precision, for example, "the height measurement of the door is 1.98 meters."
- Metametric: information about metrics….
- Metric: a measurement in relation to one or more points of reference.
- Metrication: the process of selecting and applying metrics to improve the management of something.
- Metrician: a metrics practitioner—someone fascinated with metrics who develops and uses metrics.

In Chapter 2, "Why Measure Information Security," the authors write,

From our experience, we believe there is a genuine and increasingly urgent need for

viable metrics in information security. While, to date, the profession has generally muddled through with almost no rational, sound, and defensible security measurements, the situation is simply not sustainable over the long term. We are fast approaching and, in some cases, already exceeding the limits of the information security manager's gut feeling, qualifications, and experience, coupled with the use of ill-defined and generic good or so-called best practices, as a basis for extremely important security and risk management decisions. While not so common these days, there are still those who contend that as long as you implement best practices, you don't need extensive metrics. However, best practices are an inadequate substitute for genuine knowledge. What may be best in one organization may be too costly and excessive in another or, in some cases, wholly inadequate. Without metrics, how would you ever know?

Brotby and Hinson pose and discuss the following questions in Chapter 2:

- Are we secure enough?
- Are we *more* or *less* secure than our peers?
- Which are our strongest and weakest security points?
- What are our biggest security threats or concerns?
- Are we spending (investing) too much or too little on information security, or do we have it about right?
- Are our security resources allocated optimally?
- Have we properly and adequately treated all reasonably foreseeable information security risks?
- Can we handle compromises, breaches, and other information security incidents effectively and efficiently?
- Are we (sufficiently) compliant?
- Are we *best in class*? Are we perhaps overdoing it, or are we lagging the field in information security?

They point out that metrics can help improve information security systematically: "It could be argued that we have gotten where we are today mostly through a process of trial and error, hit or miss…. If we don't even track and record incidents properly and can barely guess at which incidents are costing us the most each month or year, how can we determine which changes are truly worth making?"

Their sound arguments in Chapter 2 are consistent with the point of view expressed a decade ago in an article I called "Net Present Value of Information Security."< http://www.mekabay.com/infosecmgmt/npvsec.pdf >

Chapter 6, "Metametrics and the PRAGMATIC approach" is at the core of their method. Their PRAGMATIC metametric framework stands for these elements in judging the usefulness of metrics:

- Predictive
- Relevant
- Actionable
- Genuine
- Meaningful
- Accurate

- Timely
- Independent
- Cheap.

The authors describe a practical series of steps for evaluating metrics systematically using these objectives and include many useful tips and case studies to help the practitioner.

Chapter 7 provides a detailed application of the PRAGMATIC approach using the ISO/IEC 27002:2005< http://www.iso.org/iso/catalogue_detail?csnumber=50297 > standards for information-security management. In this example, they apply their method to "metrics measuring the processes or outcomes typically used to indicate, assess, and address information security."

Just like the approach of Computer-Aided Thematic Analysis™< http://www.mekabay.com/methodology/CATA.pdf > and Computer-Aided Consensus™,< http://www.mekabay.com/methodology/cac.pdf > the PRAGMATIC analysis serves as a *heuristic* to encourage thoughtful analysis, discussion, and development. The specific scores assigned to each component of each particular metric cannot be defined completely objectively, but thinking about them and coming to agreement are enormously useful steps in developing a rational information-assurance strategy.

Chapter 8 focuses on this question: "…[H]ow, exactly, do we establish performance measures that will derive maximum value from information security?" Using a lifecycle approach rooted in decades of experience with spiral development methodology< http://www.ianswer4u.com/2011/12/spiral-model-advantages-and.html > for systems, the authors step the readers through a cycle of stages leading to actionable metrics and preparing for the next round of improvement.

Chapter 9, "Advanced Information Security Metrics," explores lessons learned from other applications of metrics and specifically addresses the concepts and terminology for evaluating metrics, including

- High reliability
- Indicators and proxies
    - Key goal indicators
    - Key performance indicators
    - Key risk indicators
- Targets, hurdles, yardsticks, goals, objectives, benchmarks and triggers

Chapter 10, "Downsides of Metrics," takes a realistic view of what we can achieve with metrics, even the best of metrics. "…[T]here are inherent unpredictabilities with some information security metrics. We can do our level best to minimize them by using better, more reliable instrumentation and to smooth them out using … statistical techniques …, but they inevitably remain."

Chapter 11, "Using PRAGMATIC Metrics in Practice," looks in detail at sources of data, methods for analysis, data presentation, and responding to metrics.

Chapter 12 is a 40-page case study with real data anonymized for the canonical *Acme*

Enterprises, Inc. It provides detailed commentary to help the reader apply these methods to the real world.

Chapter 13 provides parting thoughts on applying these methods with strong, useful recommendations for putting the PRAGMATIC metrics into practice.

I strongly recommend this text to all information-assurance practitioners; I think it can also be useful as a textbook in graduate degrees in the management of information assurance for a specific module on metrics and optimization of security strategy.

* * *

For the record, I have no financial or professional relationship with the authors and the publisher of their text. They're just really smart and very nice folks.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

* * *