Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI
Debra S. Herrmann
Auerbach Publications, 2007
$119.95 (hardcover), 824 pp.
ISBN 0-8493-5402-1

Reviewed by Cheryl Washington

An effective performance management program can help an institution monitor and assess the effectiveness of its information security and privacy controls, policies, and procedures. Nearly all performance management programs include metrics designed to measure the degree to which people, processes, and technology protect the institution's information assets. The challenge is to select an appropriate set of metrics. One of the most common mistakes made in establishing a performance management program is to saturate the institution with metrics that have little meaning to the targeted audience. Many of us are taught that good metrics are SMART: that is, they are specific, measurable, attainable, repeatable, and time-dependent. They should also be aligned with the strategic objectives, culture, and regulatory requirements of the institution.

Complete Guide to Security and Privacy Metrics is a good reference book for individuals developing or managing metrics for performance management programs. This volume contains more than 900 ready-to-use metrics designed to measure:

- Compliance with current security and privacy regulations and standards
- Operational resilience of physical, personnel, IT, and operational controls
- Return on investment (ROI) on controls used to manage risk of information and IT assets

The book includes a comprehensive section on the what, why, how, and when of metrics. Numerous topics are covered, including a review of basic terminology and concepts, the historical and philosophical applications of metrics to information security, data collection and validation methodologies, and how to select and identify the *right* metric. This section also briefly describes the Goal Question Metric (GQM) paradigm created by Victor Basili and colleagues during the 1980s. The GQM model is a framework for measuring controls to help promote process improvement. The section concludes with references to several publications on security and privacy metrics.

A section on "Measuring Compliance with Security and Privacy Regulations and Standards" contains a wealth of information on U. S. and international regulations and standards. For anyone unfamiliar with the more well-known privacy and security regulations (including the Health Insurance Portability and Accountability Act, Sarbanes-Oxley, and the Gramm-Leach-Bliley Act), this section would serve as a good primer. For most of the regulations discussed, the author provides a historical review, allowing readers to understand the purpose of the regulation and to think about how it might apply to their institutions. The book also includes excerpts from the regulations and highlights specific controls and safeguards that can be measured. At the conclusion of each section, the author provides a set of recommended metrics that can either be used as described or adapted to meet the needs of the institution. This section contains a total of 352 metrics covering homeland security and financial, healthcare, and personal privacy regulations.

The author begins the section on developing metrics for physical, personnel, IT, and operational security controls with a discussion on resilience, which she defines as "the capability of an IT infrastructure, including physical, personnel, IT, and operational security controls, to maintain essential services and protect critical assets while preempting and repelling attacks and minimizing the extent of corruption and compromise." The book suggests that resilience metrics are required to answer two basic questions facing most institutions:

1. How secure is the institution?
2. How secure do we need to be?

The central theme of this section is that physical, personnel, IT, and operational metrics should be selected to measure the resilience of security controls that are deployed to mitigate risks. The author notes that you cannot eliminate vulnerabilities in all controls and that an appropriate strategy, therefore, is to measure how well the vulnerabilities are managed rather than whether they have been eliminated. Resilience metrics describe the strength of a control. The author suggests that if the resilience of a control is not measured, "there is no factual basis on which to make the claim that security controls are indeed commensurate with risk."

The last section in the book introduces an interesting concept involving the use of ROI modeling to develop metrics. ROI is a well-established financial model, but the author places ROI in a different context, describing a process for performing an ROI risk analysis using techniques from actuarial science to analyze the economic value of information and IT assets to calculate the probable loss and economic consequences of a security incident. Because ROI metrics are often based on the aggregation of other metrics, the development of ROI metrics should be undertaken after the performance management has matured.

To demonstrate the effectiveness of information security and privacy strategies, an institution needs to be able to measure, in quantifiable terms, the capability of controls that have been implemented to protect the institution's information assets. A performance management program that includes well-chosen metrics can help the institution monitor the outcomes and activities of its controls. This book is a useful reference for individuals who must meet the challenge of selecting good metrics.

Cheryl Washington (cheryl.washington@csueastbay.edu) is Information Security Officer at California State University, East Bay, in Hayward, California.