It is important to understand what is meant by "security metrics management." So, before we get into the details of the matter, let us define and discuss some terms.

WHAT IS A METRIC?

To begin to understand how to use metrics to support management of a corporate assets protection program (CAPP), it is important to understand what is meant by "metrics." For our purposes, a metric is defined as a standard of measurement using quantitative, statistical, and/or mathematical analyses.

WHAT IS A SECURITY METRIC?

A security metric is the application of quantitative, statistical, and/or mathenatical analyses to measuring security functional costs, benefits, successes, ailures, trends, and workload—in other words, tracking the status of each ecurity function in those terms.

here are two basic ways of tracking costs and benefits. One is by using netrics relative to the day-to-day, routine operations of each security funcon. Examples would be analyses of the costs of a security briefing program nd conducting noncompliance inquiries (internal investigations into loss of ssets). In more financial terms, these are the recurring costs.

etrics can be and are used as individual data points. They are often best ed in the depiction of trends. For example: Is the cost of security at comny X going up or down?

e other way of tracking costs and benefits is through the formal project ans. Remember that security functions are "level-of-effort" (LOE), neverding, daily work, while projects have a beginning and ending date with a ecific objective and associated discrete costs.

So, in order to efficiently and effectively develop a security metrics management program (SMMP), it is important to establish that philosophy and way of doing business. Everything that a corporate security manager and security staff do can be identified as fitting into one of these two categories: routine operations (LOE) or projects.

In other words, project plans provide project schedules and are a tool to track time and expenses in relationship to the accomplishment of a task. Both time and costs (money) are metrics in and of themselves and are included in a project plan. A project plan establishes criteria and metrics (time, costs, milestones accomplished) that are used to measure performance to plan.

WHAT IS SECURITY METRICS MANAGEMENT?

Security metrics management is the managing of a CAPP and related security functions through the use of metrics. Security metrics management is the application of an individual metric or a set of metrics as a means of assessing the performance of a security process, security processes, or an entire security program. Through the use of metrics, the security cost versus benefit analysis becomes more quantitative and easier to understand and communicate in common business terms. Metrics help the security professional and others better understand the efficiency and effectiveness (value) of an assets protection program.

METRICS, MEASUREMENT AND MANAGEMENT

Some metrics are unique to their environment—e.g., software—while others can be ported to various environments. What we are offering here for the security professional is not some scientific, complicated, or "formal" methodology that requires training classes, nor years of experience to understand and efficiently and effectively use.

What we will be discussing throughout this book is a very basic and commonsense approach to begin to get a handle on the problem of identifying costs, benefits, success, and failures of assets protection programs and their related security functions.

Parts of that, as a Chief Security Officer, you already do—budgeting, for example. What we offer is an outline—an approach—that takes the methodology of metrics measurement and the philosophy of metrics management and combines them into an SMMP. In other words, putting it all together and using it as a security management tool to manage a CAPP.

Now that you have an understanding of what we mean by security metrics management, we can move on to an introduction to business and government agency security followed by detailed discussions of developing and implementing an SMMP as an integral part of an assets protection program and its related security functions, culminating into a look into the future of business security supported by metrics.

KEY WORDS AND PHRASES

The following key words and phrases should be understood by the reader and most certainly by the security professional:

1. Security Awareness
2. Physical Security
3. Personnel Security
4. Administrative Security
5. Security
6. Computer Security
7. Information Systems Security
8. Event Security
9. Information Warfare
10. Auditing
11. Compliance Assessments
12. Managing Assets Protection
13. Managing Security Organization
14. Assets Security
15. Assets Protection
16. Information Protection
17. Privacy
18. Liability
19. Risk Assessment
20. Risk Analyses
21. Cost–Benefits Analyses
22. Measurement
23. Metric
24. Processes
25. Process Improvement